Ecole Nationale Supérieure de l'Electronique et de ses Applications (ENSEA)

Mémoire présenté en vue d'obtenir le titre d'Ingénieur Diplômé Par l'Etat (IDPE)

par

Philippe DUBOSCQ

Spécialité: Télécommunications & Réseaux

Session 2009

Support de solutions de stockage, section commutation. Cas appliqué à un client du domaine bancaire.

Soutenu le : 18 Juin 2009

Composition du jury particulier :

M.Rachid ZEBOUDJ	Maître de conférence, Président du Jury
M.Jean-Michel BERNARD	Ingénieur INSA
M.Michel CALLIER	Ingénieur DPE 2003
M.Bruno DELACRESSONNIERE	Maître de conférence
M.Daniel PASQUET	Professeur des Universités

TABLE DES MATIERES

TABLE DES ILLUSTRATIONS

1. Avant-Propos

Il paraît naturel de pouvoir consulter nos comptes bancaires via le support internet, ou encore de consulter des horaires de trains, de réserver un billet d'avion, de commander des livres, des disques, … toujours via le support internet.
Alors que, pour les utilisateurs au quotidien, il semble évident et normal d'avoir un accès immédiat et permanent à ces services, les infrastructures qui permettent ces prestations se font de plus en plus complexes et robustes. Elles incorporent des matériels sophistiqués permettant l'accès le plus rapide à un nombre de données en constante augmentation.

Si les possibilités de services se simplifient et se banalisent, il en est tout autrement des équipements qui les dispensent. En effet, les matériels, les logiciels mais aussi les protocoles qui animent ces services et par extension ces bases de données, se sont complexifiés au cours des années. C'est le cas pour les réseaux de stockage qui comme les réseaux locaux en leur temps, sont arrivés à une certaine maturité permettant des configurations extrêmement compliquées et autorisant du même coup la mutualisation des équipements, la fusion des protocoles ainsi que le regroupement des services et des activités des entreprises.

Toutefois, de la disponibilité des données dépend la pérennité et l'utilisation des ces réseaux de stockage. Il en ressort, donc, un aspect fondamental qui est la sauvegarde et l'intégrité de ces données afin d'assurer à quiconque, entreprise ou particulier qui utilise ces ressources, de pouvoir y accéder à tout moment sans risques de pertes, de corruptions ou de détériorations des informations stockées.

2. Résumé

2.1. Résumé en Français.

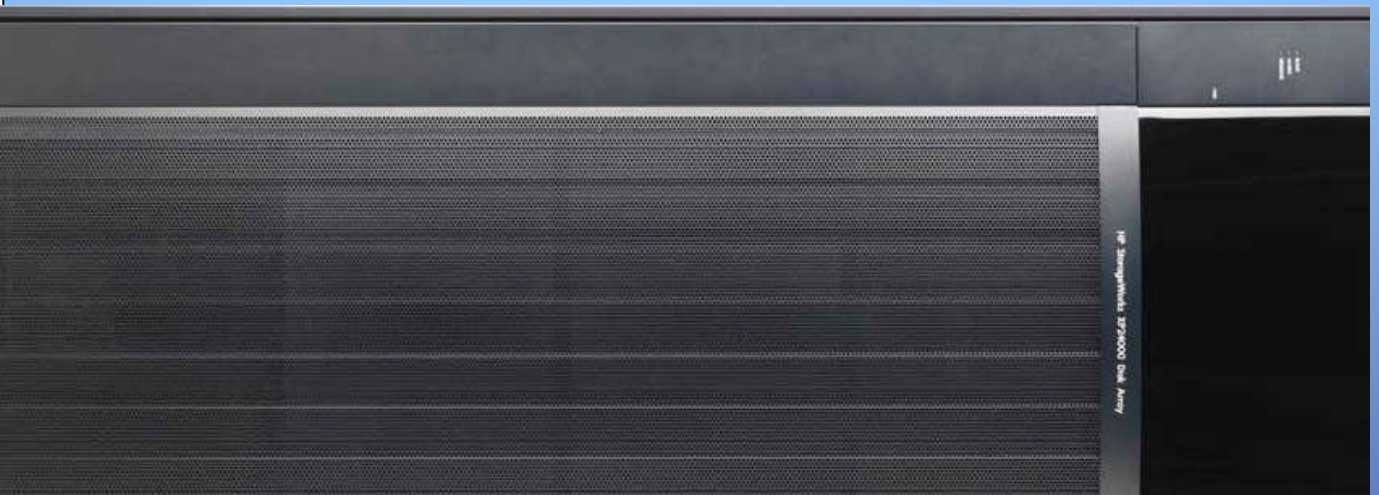
Ce mémoire traite de la gestion d'un appel au support HP, pour un client du domaine bancaire. Il s'agissait d'un problème de performance empêchant le client de pouvoir finaliser ses copies de sauvegarde sur son site de réplication distant. L'infrastructure, déployée et mise en service peu de temps avant le problème, était basée sur des commutateurs FC Cisco utilisant le réseau wan du client pour la communication intersites. Cette technologie s'appuie sur l'encapsulation des trames FC dans de le protocole IP. Ensuite, la réplication des données se fait au moyen de baies de stockage XP (matériel HP). De nombreuses investigations ont eu lieu afin de corriger le problème au plus vite, mais au final, même si plusieurs points ont été mis en avant, il n'a pas été réellement possible de mettre un seul et unique défaut en exergue. Toutefois, le principal défaut dans l'infrastructure était la possibilité pour les trames d'utiliser plusieurs chemins physiques différents avec des latences pouvant varier. Ainsi, beaucoup de trames pouvaient être reçues dans le désordre générant alors des retransmissions qui affectaient directement les performances. De plus, d'autres problèmes ont pu aussi être corrigés. Au final, quatre points ont pu être dégagés pouvant être plus ou moins liés au problème initial. Ces points peuvent être déclinés de la façon suivante : une augmentation de la quantité de données à répliquer, une anomalie logicielle et une mauvaise configuration des commutateurs MDS, enfin et surtout, une transmission sur plusieurs chemins physiques avec des latences aléatoires. A l'issue de la gestion de cet appel, l'infrastructure a donc été modifiée puis optimisée pour atteindre les meilleures performances possibles compte tenu du matériel utilisé. Après le rétablissement des sauvegardes et une période de vérification de quelques semaines, il a été possible de convenir de la correction du problème.

2.2. English abstract.

This document is talking about an HP support case for a banking customer. It was about a performance issue which prevented the customer from performing his backup on the remote site. The infrastructure implemented shortly before the problem was set up on Cisco FC switches, using the customer wan network for the inter site communication. This technology is based on the FC encapsulation in IP protocol. Then, the data replication was done using XP storage (HP vendor). Many investigations took place in order to fix the issue as soon as possible, but at the end, even if multiple points have been raised, it has not been really possible to highlight one single root cause. However, the most important issue in the network was the ability for the data frames to use multiple physical paths with different latencies. Then, lot of frames were delivered out of order which created frame retransmissions and at the end the performance was affected. Nevertheless, other troubles have been fixed as well. At the end, four aspects have been highlighted which could be more or less linked to the initial problem. These points can be shown as follows: increase in volume of data replication, firmware bug and some wrong settings in the MDS switches, and most important, data transmission over multiple physical paths with random latencies. At the end of the case management the infrastructure has been modified then optimised in order to reach the best performance possible taking into account the hardware modules in use. After the backup finalisation and a monitoring period of few weeks, it has been possible to agree on the problem correction.

Mots clefs / Key words: **SAN** – **FCIP** – **Replication** – **FC** – **Cisco** – **MDS** – **Support**

PARTIE A – GENERALITES



3. Introduction

3.1. Introduction du mémoire

Les demandes de stockages de données dans les entreprises ne cessent d'augmenter et, avec elles, l'importance de les sauvegarder dans un lieu sûr et sécurisé. Tous les secteurs d'activités sont concernés : banques, assurances, santé, industries, services publics,… toutes les sociétés, quelle que soit leur taille ont besoin de sauvegarder leurs informations. Ces données peuvent être très diverses, allant des factures d'usagers aux fiches de paies d'employés, mais aussi aux transactions bancaires, contrats d'assurances, études et recherches, bon de commandes, réservations … Pour toutes ces activités, les informations à sauvegarder sont primordiales pour leurs utilisateurs et il n'est pas concevable de les perdre. Cette demande de disponibilité ne cesse de s'accroître obligeant les équipements à fonctionner constamment [1] (ce qui est très difficile à assurer au vue des mises à jour logicielles, des interventions ou des pannes matérielles,…) ou bien à multiplier les équipements qui sont impliqués dans le réseau afin d'assurer une redondance.
La gestion et les besoins de stockage de données sont des tâches importantes, gérées généralement par les administrateurs réseaux des entreprises, n'acceptant pas ou peu la perte d'informations. Toutefois, pour certaines sociétés, il est absolument impossible de perdre des informations, ne serait-ce qu'une partie, car de leur disponibilité dépend la survie de ces entreprises. Tel est le cas, par exemple, du domaine bancaire. En effet, toutes les transactions sont stockées et mémorisées quotidiennement. Si, en cas de problème technique majeur[2], il y a une dégradation des données, alors, la conséquence financière est immédiate et se traduit par une perte sèche pour la banque et ses clients. De plus, il en résulte un très grave problème de sécurisation, point important de la confiance accordée à une banque.

Ce mémoire traite de l'appel support 1600381090 enregistré le 18 Mars 2008 au support HP, pour un problème de réplication [3]de données pour un client du domaine bancaire. D'un abord simple et peu pénalisant pour les applications du client, cet appel est très vite devenu hautement critique et m'a donc ensuite été élevé, lors de mon astreinte, avec une formulation peu précise de la problématique.
Il faut savoir, que cette toute nouvelle infrastructure avait été installée et mise en service quelques mois auparavant suite à un appel d'offre remporté par HP services.

De part cet historique et du fait que la situation du client était critique, il a fallu que l'organisation support toute entière fournisse un service exceptionnel afin de résoudre la crise au plus vite, ceci permettant de fixer le problème du client et de lui prouver la fiabilité des matériels et services HP.

Le mémoire présente dans une première partie, l'importance du client, ses besoins en termes de stockage ainsi que les choix optés lors de la mise en œuvre du projet. Quelques concepts de stockage y sont également abordés.
La seconde partie traite de l'appel support, en faisant apparaître les conséquences directes sur le client et ses partenaires. Les aspects techniques et les défauts rencontrés puis corrigés y sont développés. De plus la méthodologie et les différentes actions menées y sont étudiées et analysées rétrospectivement avec des propositions afin d'optimiser la solution en place.

[1] « 5 nines reliability » : 99,999% du temps disponible, soit 5min d'indisponibilité par an.
[2] La notion de problème technique majeur signifie un événement interne ou externe conduisant à une panne grave sur l'infrastructure. Ces problèmes peuvent être d'ordre climatique, terroriste, erreurs humaines, …
[3] Réplication : copie des données depuis un site local vers un site distant.

Enfin, la troisième partie concerne, entre autre, ma conclusion personnelle : ce que m'ont apporté cette intervention, la rédaction de ce mémoire et plus globalement le cursus IDPE.

Pour information, le client assurait lui-même le support de la partie réseau (pas de contrat avec HP pour ses équipements). De plus, du fait de ma spécialité (support commutateur FC), les baies de stockage, les serveurs et les équipements réseaux (routeurs, commutateurs clients) ne feront donc pas partie de l'analyse détaillée, même si évidemment il en sera question dans le mémoire. Il sera donc traité dans le mémoire essentiellement des aspects de commutations FC. D'autre part, l'équipe de gestion du compte client m'a demandé de garder confidentielles certaines informations liées au client (son nom,…).

3.2. Concepts et généralités

3.2.1 Plan de Secours Informatique et Plan de Continuité de l'Activité.

Le Plan de Secours Informatique (PSI) comprend tous les moyens techniques mis en place afin de garantir le redémarrage des applications critiques après un sinistre informatique ou après tout événement qui aurait mis en péril les données. Cette notion de PSI, fait partie d'un plan d'actions plus vaste qui est le Plan de Continuité de l'Activité ou PCA. Le PCA, quant à lui, englobe plus largement toutes les actions à mener afin de permettre un retour à la normale de l'activité de l'entreprise (locaux disponibles, alimentation électrique, personnel d'astreinte, matériel informatique,…). Du processus mis en place pour récupérer les données conforme aux besoins du PCA dépendra l'infrastructure utilisée. Dans la plupart des cas, les installations informatiques comportent un site jumeau, éloignés de plusieurs kilomètres, permettant la sauvegarde des données en lieu sûr, très probablement non impacté en cas de problème critique sur le site principal. Les normes telles que BS25999, ISO20000, ISO27001 traitent de ces problèmes de sécurisations des données informatiques et plus globalement de la gestion de la continuité des activités.

3.2.2 Les Backup

Globalement, on entend par « backup » l'action de dupliquer des données, principalement sur un support physique différent. En effet, les données sont habituellement enregistrées dans des mémoires, de capacités diverses. Ensuite, le backup a pour but d'enregistrer ces données sur un support physique généralement non altérable et indépendant de son alimentation électrique, tel qu'un disque optique, une bande magnétique,…
Dans les environnements de stockage, le backup se fait par l'intermédiaire d'un serveur qui pourrait être schématiquement défini comme une pompe, qui prendrait les données depuis un support pour les copier sur un autre type de support.

Toutefois, on peut aussi parler de backup quand on duplique les données sur un même type de support, comme, par exemple, copier les données d'une baie de stockage sur une autre baie de stockage de même support physique.

3.2.3. Les Baies de stockages

Les baies de stockages peuvent être vues comme de simples disques durs reliés entre eux, formant un gigantesque disque dur virtuel pouvant atteindre des tailles impressionnantes atteignant les Péta Octets (10^{15} octets). L'intelligence de ce disque est gérée par un serveur externe (ou plusieurs serveurs dans le cas de redondance). Ce serveur permet de « découper » cet énorme disque dur virtuel en de plus petites zones mémoires utilisables par d'autres serveurs ou PC et qui sont vues comme de simples espaces disques. Ce disque dur virtuel, peut donc être augmenté ou diminué en ajoutant ou retirant des disques durs physiques et les espaces mémoires être modifiés à l'aide du serveur qui gère ces baies de stockages.
Toutefois, ce type de stockage nécessite une modification de l'infrastructure afin d'offrir toutes ces possibilités. En effet, l'intérêt est de pouvoir avoir de multiples serveurs pouvant accéder aux baies de stockages quelle que soit leur localisation physique. Un intérêt supplémentaire est de pouvoir intégrer plusieurs baies de stockage afin d'augmenter la redondance de l'infrastructure. Pour répondre à ces besoins, il faut alors utiliser une infrastructure basée sur la commutation.

3.2.4 La commutation

La commutation implique une modification de l'architecture car, avec ce système, il n'est plus possible de connecter les équipements un a un, comme en topologie [4] « attachement direct [5] ». Il faut permettre à plusieurs serveurs d'accéder à plusieurs baies de stockages partagées en évitant des coûts d'infrastructures exorbitants. Ainsi, les infrastructures basées sur la commutation ou le routage sont déployées pour répondre à cette demande.

La commutation est un terme générique, ce concept est le même quels que soient les protocoles utilisés. Toutefois, un commutateur dédié à un protocole ne pourra pas forcément reconnaître et traiter des trames d'un autre protocole, pour lequel il n'est pas configuré.
Un commutateur peut être vu comme un équipement central sur lequel les serveurs et baies de stockages sont connectés. Cet équipement fait le tri entre les différentes demandes d'accès depuis les serveurs vers les baies. Ceci assure une évolutivité de l'infrastructure en ajoutant ou retirant des serveurs, des baies de stockages, mais aussi en l'interconnectant à d'autres commutateurs. Le commutateur permet donc une très grande souplesse dans la gestion de l'infrastructure. De plus, ces commutateurs peuvent assurer d'autres rôles tels que la sécurité, en définissant des règles d'accès pour chaque serveur ou en isolant certains types de trafics. Ils permettent également des interconnections sur de très longues distances, peuvent agir comme des interfaces d'un point de vue protocole,…

Actuellement, les constructeurs de commutateurs FC ne cessent d'ajouter des fonctionnalités. Ces produits sont de plus en plus sophistiqués et permettent des designs et des options des plus élaborées. L'un des constructeurs émergents sur ce segment de marché est Cisco System avec la gamme de produit MDS (Multilayer Datacenter Switch) qui est la gamme de commutateur Cisco SAN[6]. Dans le présent document il ne sera traité que de ce constructeur étant donné que l'infrastructure du client ne comportait que ce type de produit.

[4] Topologie : disposition logique des éléments composant le réseau et de leurs interconnexions.
[5] Direct Attach : un serveur accède à un ou plusieurs équipements de stockage directement connectés.
[6] SAN : Storage Area Network – réseau haut débit dédié au stockage.

3.2.5 Encapsulation

L'encapsulation est le terme générique du processus permettant d'insérer des données ou un protocole dans un autre protocole. Chaque protocole possède ses propres en-têtes et traînes. Ainsi, chaque couche successive ajoutera son en-tête et, suivant le cas, une traîne supplémentaire et ainsi de suite jusqu'à la couche physique. Ensuite, une fois que la trame arrive à l'autre extrémité, l'opération inverse s'effectue. Il s'agit de la « dés-encapsulation » qui, successivement, permettra de retrouver les données d'origine pour leurs traitements par l'application finale. Ci-dessous un schéma représentant l'encapsulation successive des données d'un protocole vers un autre protocole.

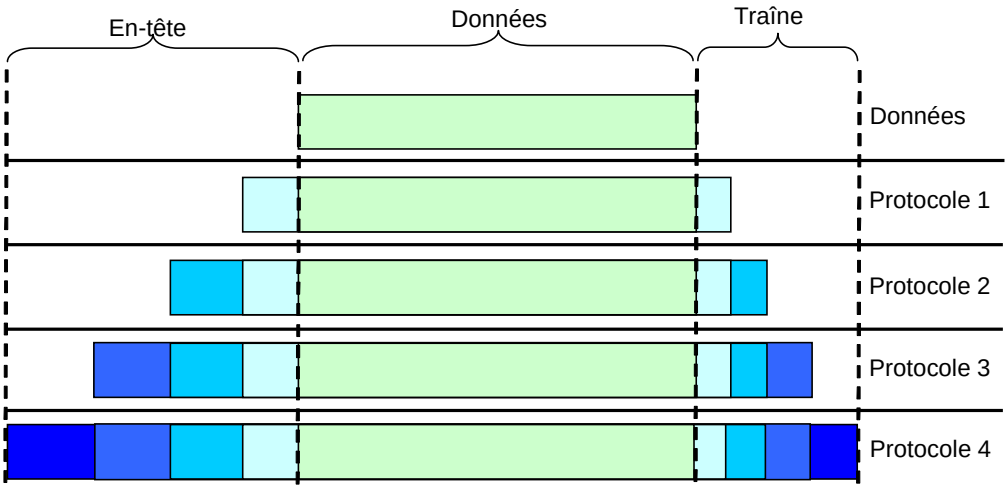


Figure 1: Illustration de l'encapsulation

Dans le présent dossier, il sera traité d'un problème incluant l'encapsulation du trafic Fibre Channel dans un réseau Ethernet. Cette opération est appelée FCIP, car la trame FC est d'abord encapsulée dans les protocoles TCP/IP avant d'accéder à la couche Ethernet.

3.2.6 Exemple de solutions incluant des commutateurs FC

Dans le monde du stockage, les infrastructures sont généralement redondantes, pour que les applications cruciales puissent être plus tolérantes à des actions de mise à jour de l'infrastructure ou bien à des pannes. En effet, l'utilisation d'équipements redondés permet d'intervenir sur une partie de l'infrastructure sans perturber l'autre partie et ainsi permettre aux activités de continuer sans être gênées.

Une fabric est un SAN où sont interconnectés les serveurs, équipements de stockage et commutateurs, routeurs,… Il est donc habituel d'utiliser deux fabrics afin de former une infrastructure redondante. C'est ce que l'on appelle une infrastructure « dual Fabric [7] ».

Dans les SAN de tailles importantes, il est préférable d'utiliser une infrastructure de topologie « core-edge[8] » ; elle met en avant des commutateurs appelés « Edge » qui ont pour mission de connecter des serveurs et équipements de stockage, qui sont eux- même interconnectés au

[7] Dual-Fabric : Double Fabric.
[8] Core-Edge : « Core » signifie « cœur » dans le sens d'équipement centralisé et « Edge » signifie « bord », dans le sens d'équipement d'extrémités.

travers d'un ou plusieurs commutateurs « Core ». Ces commutateurs Core sont généralement de gros commutateurs aux performances élevées permettant un nombre de connexions important. Les commutateurs de types Edge sont, quant à eux, généralement de taille plus modeste. L'intérêt de ce type de topologie réside en une harmonisation des principes de connexion et d'ingénierie. Elle empêche aussi, dans un objectif de performance, une évolution anarchique de l'infrastructure, en évitant de mettre en série trop de commutateurs. En effet, ceci est néfaste pour la propagation des changements de configuration dans la fabric et pour les performances en termes de trafic.

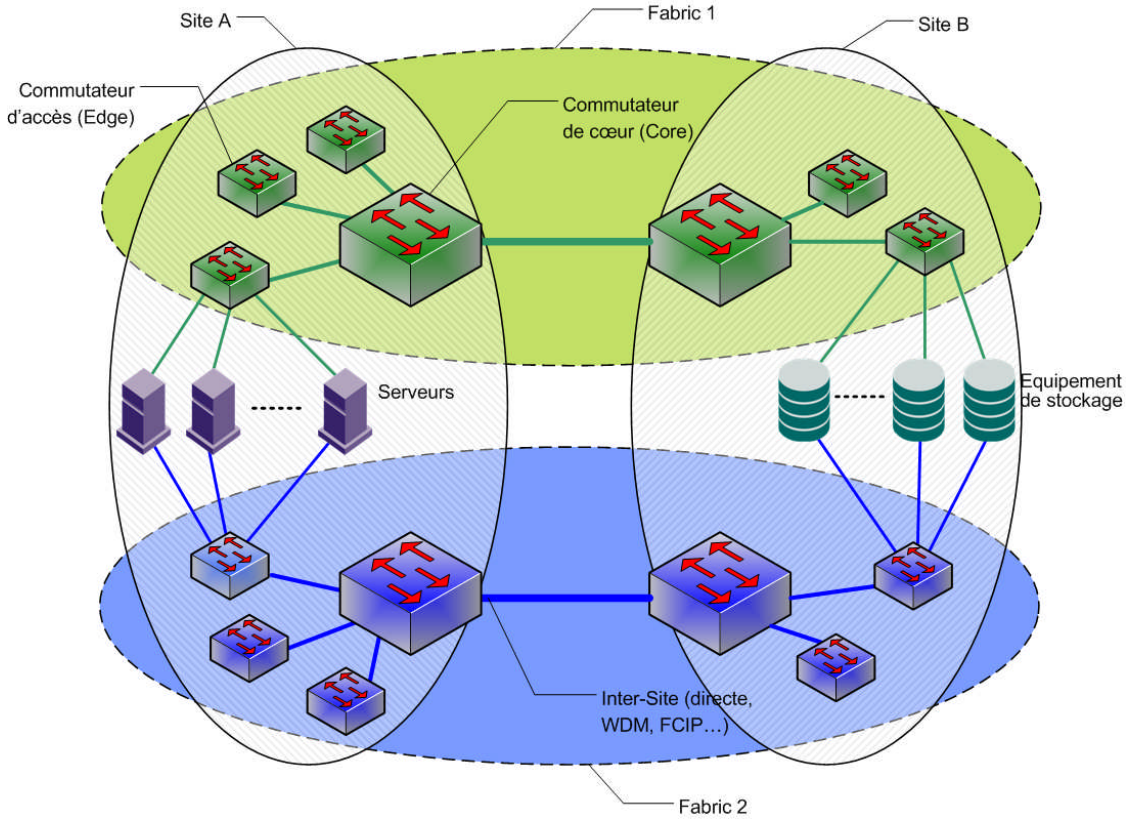


Figure 2: Exemple de la composition d'un SAN.

4. Présentation

4.1. Le client

4.1.1. Présentation du client

Le client, pour lequel l'appel a été ouvert, fait partie d'un groupe bancaire international privé. Son poids financier (80Md€ d'actifs et 1Md€ de bénéfice), le nombre élevé de ses collaborateurs (20000) et sa présence importante en Europe, notamment en Europe Centrale et en Europe de l'Est font de ce client un acteur majeur dans le domaine bancaire. De plus il est implanté dans une zone géographique où l'émergence économique développe un climat de concurrence très élevée. Ainsi, sa position dominante et la situation concurrentielle dans laquelle il se trouve font que ce client est très soucieux de la qualité de son infrastructure et des services fournis.

4.1.2. Les besoins du client

Les besoins de ce client en termes de volumétrie sont conséquents. Il a été estimé, lors de la réponse à l'appel d'offre, que les besoins en données répliquées étaient d'environ 14To à l'issue de la mise en œuvre du projet avec une augmentation annuelle approchant 4To. Aussi, la répartition géographique des sites devait être restructurée, afin de consolider l'infrastructure autour de deux sites principaux éloignés de plusieurs centaines de kilomètres l'un de l'autre. Les besoins en termes d'objectif de récupérations étaient les suivants :

► Durée de la récupération des données

Cette notion est désignée par le RTO (Recovery Time Objective) qui définit le temps maximal qu'il faudrait pour le rétablissement des applications en cas de sinistre informatique. Cette notion est déclinée par type d'applications.

► Quantité de données perdues

Cette notion est désignée par le RPO (Recovery Point Objective) qui définit la quantité acceptable de données perdues depuis la dernière sauvegarde. Ainsi, pour les activités Business Critical et Business Enabling les sauvegardes ont lieu 1 ou 2 fois par jour. Pour ce qui est des applications Mission Critical, la perte devra correspondre au temps qu'il faut pour répliquer les données d'un site à l'autre, soit approximativement 500ms au maximum. Ceci signifie que ces applications copient en permanence les données sur les deux sites simultanément.

Classification des applications	Recovery Time Objective	Recovery Point Objective
Mission Critical (MC)	**≤ 4h**	**≤ 500ms**
Business Critical (BC)	**≤ 12h**	**≤ 12h**
Business Enabling (BE)	**≤ 24h**	**≤ 24h**

Figure 3: présentation des besoins du client.

4.2. Le projet

4.2.1. Enjeux

Cet appel d'offre faisait suite à un problème très grave qui avait, l'année précédente, affecté directement la disponibilité des données du client. Il fallait donc pouvoir élaborer une proposition pouvant réellement pallier ce type de problème technique et répondre totalement aux contraintes liées aux activités du client. Une des contraintes était le temps de latence entre les deux sites, induit par une infrastructure longue d'environ 2000km.

4.2.2. Solution technique adoptée

L'infrastructure entre les deux sites engendre une latence au minimum de 10ms en aller-retour (uniquement pour le temps de parcours du signal dans la fibre). Si à cela on ajoute les latences des équipements, … on peut atteindre des valeurs de 8 à 10 fois supérieures. Depuis, il a été mesuré en conditions réelles que le temps de parcours du signal en aller-retour était compris entre 70 et 120ms. Ainsi, ces données ne pouvaient autoriser l'utilisation de réplication synchrone. Il fallait donc utiliser une technologie permettant la réplication asynchrone mais avec une bande passante élevée et une bonne stabilité sans engendrer des coûts d'infrastructure exorbitants. Pour la commutation intersites, il a donc été décidé d'utiliser l'infrastructure réseau du client, en augmentant la bande passante. Les commutateurs utilisés devaient supporter la fonctionnalité FCIP. Le choix du constructeur s'est porté sur Cisco qui propose la gamme de produits MDS.

Au total, l'infrastructure contient environ 200 ports utilisés pour la connexion des équipements (170 serveurs et 30 ports pour les baies de stockages). Ces matériels sont interconnectés au travers de commutateurs MDS, deux par sites (un dans chaque fabric). La connexion intersites étant réalisée en utilisant la fonctionnalité FCIP. Sur chaque site, il y a aussi une baie de stockage XP12000 avec une capacité de stockage de plusieurs Téra octets, la réplication entre les deux baies se fait par le Continous Access (CA). Le CA est une fonctionnalité HP pour la copie directe entre les baies de stockages.

4.3 Le support HP

4.3.1. Organisation de la structure support

Le recours au service de support HP s'effectue sous la forme d'un appel auprès du Centre de Coordination des appels regroupé par pays. L'accès à ce centre s'effectue par téléphone ou par WEB. Un identifiant est communiqué à chaque client HP. Il est demandé pour l'enregistrement de chaque demande d'intervention. Lors de l'enregistrement de l'appel, un numéro de dossier unique est créé et fourni au client. Ce numéro pourra servir ultérieurement de clé si l'utilisateur rappelle au sujet de ce même problème.
L'appel est automatiquement transféré dans le système HP de suivi des interventions. Cet outil est utilisé par l'ensemble des services supports pour le suivi des opérations (quels que soient la technologie ou le pays). En fonction du niveau de service et dès la création du dossier, la date et l'heure sont mentionnées, elles servent de base à la mesure du respect des engagements contractuels. En effet, une fois enregistré, l'appel est suivi en permanence jusqu'à sa résolution finale. Un statut est affecté au dossier à chaque étape du traitement. Son évolution au cours du temps permet de suivre le bon déroulement des opérations.

Des alarmes, automatiquement positionnées sur ce dossier, permettent de contrôler le bon déroulement de la procédure, le respect des engagements et la « traçabilité » des interventions. Elles se déclenchent dès qu'un niveau de service ou un délai contractuel risquent de ne pas être respectés. Si l'appel n'est pas pris en compte dans les délais, le management en est averti et déclenche les actions à mener pour rétablir une situation satisfaisante.

Cette première étape, n'est en rien technique, elle a pour but de qualifier l'appel avec le client et, ensuite, d'orienter cet appel dans l'équipe support correspondante. A ce stade de la gestion du problème, l'appel est transféré au support Niveau 1 (N1). C'est ce niveau de support qui, ensuite, gérera, dans les cas les plus simples, la communication avec le client et fournira les réponses techniques aux problèmes précis (dépannage, expédition de matériels de remplacement, demande d'intervention ingénieur sur site,…). Le support N1 est organisé par pays et par technologies. Il ne fournit pas d'analyse niveau expert, mais plutôt une analyse avec une approche « solution ». En effet, chaque technologie couvre de larges gammes de produits, il est donc très difficile de maintenir à jour une connaissance experte sur tous les équipements d'une technologie particulière. Ainsi, une approche plus globale, dite par solution, permet au support N1 d'analyser globalement le problème et de le comprendre. Si le premier niveau de support n'est pas dans la capacité de résoudre le problème, alors l'appel est élevé au niveau de support supérieur (Niveau 2 ou N2). Le rôle du N1 est alors d'orienter l'appel dans l'équipe N2 adéquate avec les informations nécessaires.

Ce support N2 est spécialisé par gamme de produit dans une technologie précise, comme par exemple baies de stockage XP, réseau, serveur HP-UX. Il est regroupé par zones géographiques, le monde étant découpé en trois zones : APJ, EMEA et AM[9]. Dans mon cas, je suis ingénieur support N2 pour les commutateurs Fibre Channel dans les environnements SAN sur la zone EMEA. Le N2 doit être capable de fournir un plan d'actions détaillé au N1 qui le communiquera au client. Dans les cas plus compliqués, le N2 peut prendre en charge directement la communication avec le client.

Si, pour diverses raisons, le support N2 a besoin d'assistance technique, il est possible d'élever l'appel au service Ingénierie, généralement basé aux Etats-Unis. Ce niveau de support, appelé Niveau 3 (N3) est en relation avec les constructeurs. Le N3 est une équipe spécialisée par gamme de produit dans une technologie (comme le support N2) mais elle gère les appels à un niveau mondial. (Le N3 reçoit les élévations des N2 des zones APJ, EMEA et AM). En cas d'élévation au N3, le support N2 est responsable de la communication depuis le N3 vers le N1 ou avec le client directement.

Enfin, dans les cas graves nécessitant un traitement particulier ou ayant un impact commercial fort, il est possible de mettre en place une organisation à même de gérer une situation très complexe : une escalade. Ce processus permet de gérer un problème technique très compliqué nécessitant l'implication de plusieurs équipes N2 et N3. Une escalade met en place une cellule de crise qui est composée du personnel support technique, généralement N1, N2 et N3 ainsi que le management. De plus, un manager dit « d'escalade » intervient afin de s'assurer que tous les intervenants sont au même niveau d'information, que chaque personne fournit le travail nécessaire et répond dans les temps aux questions qui lui sont posées.

L'escalade pilotée par le manager d'escalade implique aussi le responsable du support de compte client et le responsable du service de compte client. le responsable du support de

[9] APJ (Asia Pacific & Japan), EMEA (Europe Middle East and Africa), AM (América)

compte client est un point de contact privilégié entre le client et l'entreprise HP afin de gérer les aspects support. Ce responsable de compte connaît bien l'historique lié au client et connaît aussi les conditions et l'environnement dans lesquels se déroule l'appel. Le responsable du service de compte client, interagit à un niveau de management supérieur, gère tous les aspects du compte, qu'ils soient de service pro-actif, curatif, légal ou contractuel. Dans l'appel traité dans ce mémoire, ces personnes étaient aussi impliquées durant toute l'escalade.

4.3.2. Les différents services / contrats

Le service Maintenance des équipements est un service curatif matériel pour les produits HP ou non, tous étant supportés par HP. Ces services peuvent avoir les caractéristiques suivantes :

-Période de service : de 8h à 24h par jour sur 5 ou 7 jours par semaine
-Maintenance standard avec délai d'intervention sur site : en J+1 ou 4 heures
-Maintenance avec Délai de Réparation Garanti (DRG) dans un délai très court.

Ces services engendrent certains engagements, tels que l'intervention humaine ou l'engagement de réparation sur site dans les délais contractuels, ainsi que les procédures d'escalade et des structures de haute disponibilité dans l'organisation support HP (management, techniciens et ingénieurs).

4.3.3. Organisation de la structure support lors de l'escalade traitée

Même si le processus d'escalade est standardisé, il est suffisamment souple pour pouvoir s'adapter à toutes les situations. En effet, chaque appel à sa propre complexité liée à des aspects multiples, comme le caractère critique, l'historique du problème ou du client, les contrats en cours,…
La figure 4 représente le schéma de communication lors de l'escalade traitée dans ce mémoire. Je tenais un rôle actif dans trois équipes (expert technique, escalade et technique client). Les flèches indiquent les obligations de communiquer. Elles sont soit procédurales soit contractuelles. Par exemple, le fournisseur du service « réseau WAN » n'avait de relations qu'avec le client, car d'un point de vue contractuel, il n'avait pas à rendre compte à la société HP. De même l'ingénieur du support Cisco était uniquement en relation avec HP et n'avait pas officiellement de contact avec le client final. Toutefois, suivant les besoins (ponctuels) il est possible de faire communiquer les différents intervenants afin de simplifier et faciliter le dépannage.

Lors de cette escalade et du fait des intervenants, j'ai pris une place très importante dans la communication et l'analyse du défaut. En effet, le service ingénierie et le Support TAC étant basé aux Etats-Unis, avec 6h de décalage horaire, je me suis trouvé être le seul membre de l'équipe des experts technique SAN à travailler sur la zone européenne. Le problème étant lié à un environnement de stockage, l'ingénieur N2 réseaux ne pouvait s'impliquer que dans la partie exclusivement réseau. Ainsi, j'étais le plus qualifié pour avoir le rôle de leader dans la communication technique. Mon rôle consistait donc à participer aux réunions téléphoniques, à répondre aux questions du client, à analyser les logs des commutateurs, à fournir et suivre les plans d'actions.

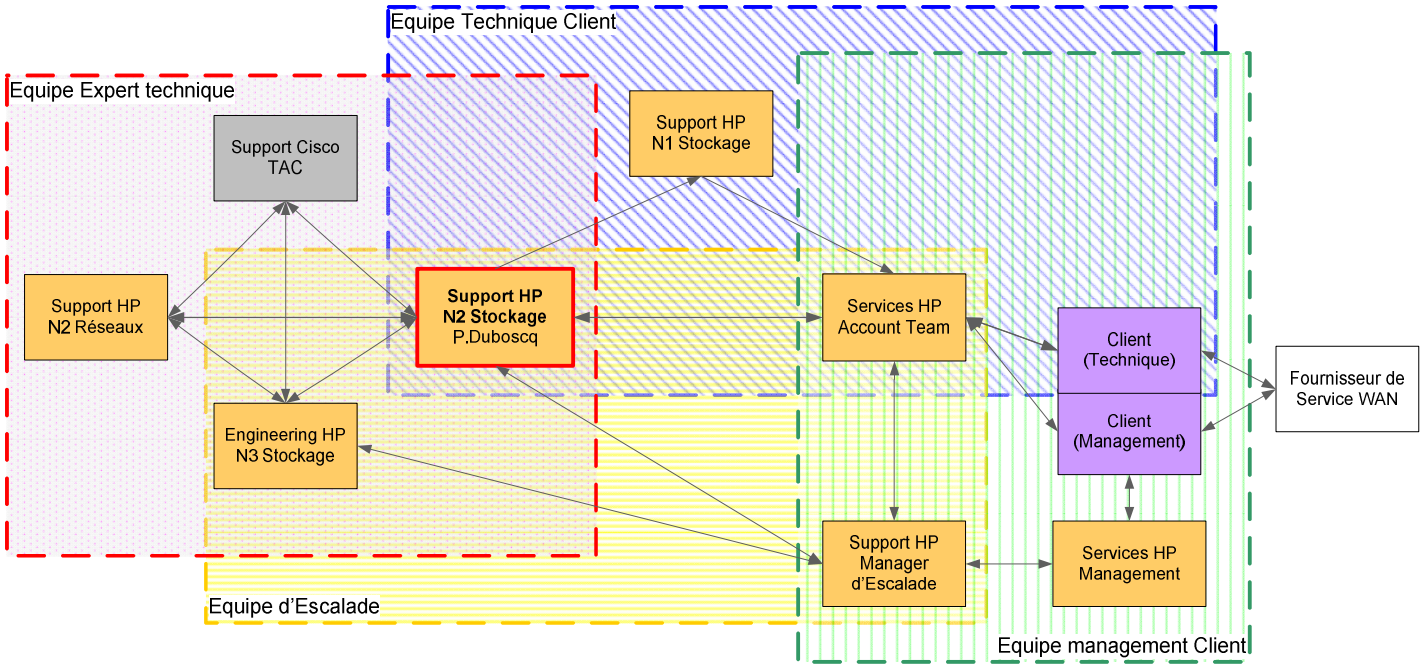
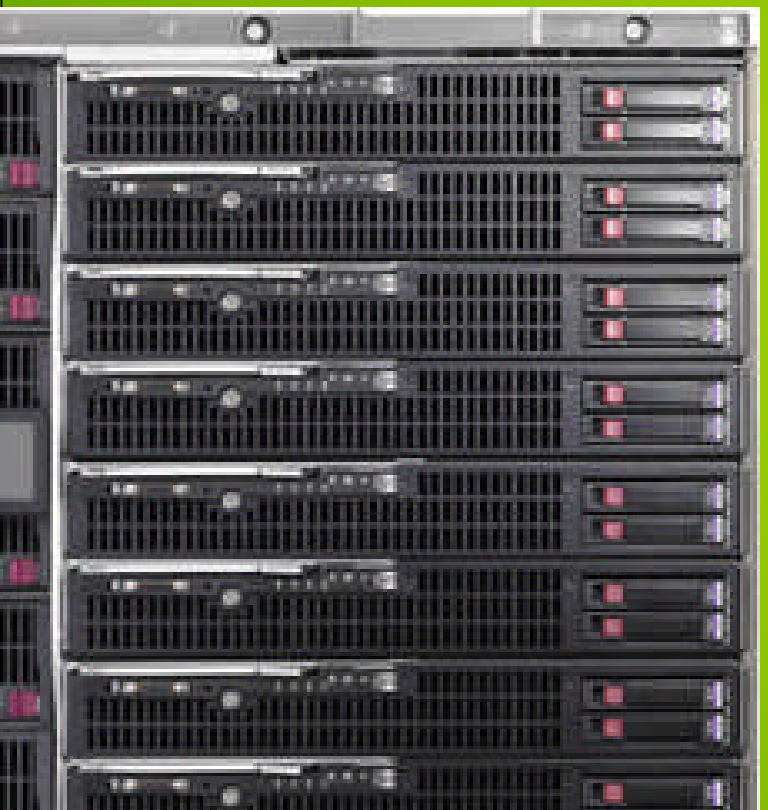


Figure 4: Schémas représentant les échanges lors de l'escalade.

PARTIE B – CAS APPLIQUE



5. Problématique

5.1. Problème rencontré

L'appel tel qu'il a été ouvert au début, était un problème de réplication des données entre les deux sites DR[10]. Le défaut présenté de cette façon, le support de premier niveau n'a pas été alarmé, en effet, l'impact sur la sauvegarde des données ne s'était pas encore fait ressentir et le client n'avait pas encore été affecté. L'appel était donc traité avec une priorité medium ne nécessitant pas d'actions immédiates ni d'implications de l'équipe d'astreinte. Puisque le niveau de criticité d'un appel est défini en accord avec le client, cela signifie aussi qu'a l'ouverture de l'appel, ni le client, ni le support HP ne s'était rendu compte des dommages potentiels pouvant apparaître. Toutefois, quand les copies de sauvegarde ont débuté, un grand nombre de backups n'étaient plus synchronisés, empêchant la copie sur le site distant. Ce problème devenant critique pour l'intégrité des données du client, la priorité a donc changé, les responsables HP de ce client ont été immédiatement contactés et l'appel a été élevé à mon niveau de support.

J'ai tout d'abord travaillé sur la redéfinition exacte du problème, avec la collaboration des différents intervenants (client, support N1 et responsables de compte), afin de mieux cerner le travail qui était à fournir par la suite. Bien que cette tâche puisse paraître une perte de temps dans les premières heures de l'appel, cette définition est, de mon point de vue, essentielle dans l'analyse, car elle permet de savoir sur quels éléments il va falloir s'orienter en premier lieu. Il faut bien noter qu'à ce moment de l'appel, seul le client est sur le site. Il est le seul à connaitre son infrastructure, comment elle fonctionne et comment elle doit se comporter. C'est également le seul intervenant qui est au courant de tout l'historique lié à son matériel, tel que son évolution, les modifications récentes. Ainsi, après discussion, j'ai pu définir le problème de la façon suivante :

Il s'agit d'un problème de performance aigu n'impliquant pas un arrêt de la production client, mais ne permettant plus la copie des données entre les sites de réplications.

Comme il n'y avait pas d'arrêt de production, cela signifiait que les deux fabrics fonctionnaient et que les applications courantes ne souffraient pas du problème. Par contre, le problème allait être complexe à corriger, étant donné qu'un problème de performance peut venir d'éléments multiples.
En effet, un arrêt de production dû à une coupure franche de la liaison intersites est assez simple à détecter, même si la correction peut en être difficile. Il est important d'être capable d'appréhender le problème dans les logs, car on sera alors capable de confirmer avec de nouveaux logs si le problème est résolu.
Cependant, un problème de performance peut être un ralentissement dû à la réduction de bande passante, à des erreurs sur une connexion, une application défaillante, … tous ces problèmes sont plus durs à identifier au travers des logs et donc plus difficiles à dépanner. Avant de proposer un plan d'actions pour corriger un défaut, il faut être capable de définir et de comprendre ce défaut, sinon, le plan d'actions risque d'être trop vague, obligeant les intervenants à de multiples actions, qui, si elles sont trop nombreuses, peuvent ne pas être faites dans leur totalité. Le risque est donc de passer à côté du problème et de faire perdre du temps au client. Ceci engendre un mécontentement, la perte de confiance dans l'analyse et la gestion de l'appel.

[10] DR (Disaster Recovery) : un site DR est un site distant du site principal permettant le redémarrage des activité en cas de sinistre informatique.

5.2. Risques pour le client

Une fois le problème défini avec précision, il est plus facile de comprendre les conséquences potentielles. Le risque majeur pour le client était une incapacité de synchroniser les sauvegardes des transactions bancaires de certains pays, particulièrement pour les plus importants, celles pour lesquelles les données à transférer sont les plus conséquentes en termes de volumétrie. Cette impossibilité de copie signifiait que les données n'étaient disponibles que sur un seul et unique lieu de stockage, induisant un haut risque de perte d'information en cas de problème sur ces équipements (panne de courant, panne matérielle, erreur humaine,…).
Le problème n'avait pas de conséquences directes sur les activités du client, en effet la production n'était pas affectée. L'activité bancaire continuait de fonctionner normalement. Le risque était que durant toute la période d'analyse et d'action, période durant laquelle les sauvegardes ne pouvaient être finalisées, toutes les données enregistrées depuis la dernière sauvegarde soient perdues en cas de défaut majeur sur le site principal. Ainsi, plus le temps passait, plus la quantité de données à transférer augmentait et plus la possibilité de faire les sauvegardes se réduisait.
Mécaniquement la criticité de ce problème augmentait avec le temps et, parallèlement, l'insistance du client pour résoudre cette crise au plus vite. Ceci se traduisait par une très forte tension au sein de l'organisation support.

Le fait que cette infrastructure était récente avait aussi toute son importance dans la gestion de l'appel. En effet, l'installation qui venait d'être finalisée quelques mois plus tôt, suite à un appel d'offre remporté par les équipes projets d'HP, avait pour but la refonte de l'infrastructure afin d'assurer l'intégrité des données. L'environnement du client était donc quasiment neuf et devait répondre aux exigences de design (performance, robustesse et évolutions,…) présentées par les consultants lors de l'appel d'offre. D'autant plus que cet appel d'offre était la conclusion d'un autre problème, issu d'une panne majeure qui avait généré une perte de données pour le client l'année précédente. Le client avait donc décidé d'investir une somme conséquente dans son infrastructure informatique afin de ne plus rencontrer de problème de ce genre. Avec cette nouvelle perturbation et l'incapacité de finaliser les sauvegardes, il se retrouvait une nouvelle fois dans la situation qu'il avait rencontrée un an auparavant. Face à elle, son inquiétude augmentait logiquement.

5.3. Définition du critère de résolution

Comme la définition du problème, la définition du critère de résolution est toute aussi importante. En effet, une fois le défaut compris et l'orientation de mes recherches définie, il faut trouver ce qui permettra de confirmer que le problème est corrigé.
Dans le cas d'une coupure franche ou d'un équipement qui aurait subi une défaillance temporaire, il est assez facile de déterminer quel sera le critère de résolution. Il peut être, par exemple, la confirmation de l'origine de la panne ou la correction du défaut temporaire. Néanmoins quand il s'agit d'un problème de performance, la définition est plus délicate à exprimer. Dans le cas présenté, même une fois les réplications réactivées, il n'est pas certain que le problème réel soit résolu. Suivant l'évolution de l'infrastructure (augmentation de la volumétrie à répliquer et du besoin de bande passante…), on peut très bien ne s'apercevoir d'un défaut qu'après la réactivation des réplications. Il faut donc pouvoir connaître les performances avant le défaut et, en même temps, découvrir à quel moment est apparu ce problème de performance. On ne peut donc pas se baser sur les valeurs présentées depuis la

mise en œuvre du projet. Ce fut le cas avec cet appel. Il a fallu s'appuyer sur les chiffres théoriques afin de confirmer le critère de résolution. Ce dernier apparaît ainsi :

L'appel sera défini comme résolu lorsque les réplications fonctionneront sans problèmes de performances, à pleine charge et ce durant une période de surveillance d'un mois. De plus, les origines de ce problème seront définies et corrigées, afin d'atteindre potentiellement la valeur maximal de la bande passante disponible dans l'infrastructure.

Cette définition du critère de résolution n'est pas officiellement édictée lors de l'ouverture d'un appel. Elle n'est souvent formulée qu'à la fin de la gestion du problème, quand arrive le moment où l'on s'interroge sur les réponses fournies et celles qui restent à fournir. Toutefois, dans cet appel, la nécessité de formuler le critère de résolution est apparue assez tôt afin de bien distinguer ce qui relevait purement du dépannage et des actions correctives, de ce qui relevait des propositions de design (incombant moins aux équipes supports qu'à celles de consulting). Cette définition a, donc, son importance pour bien identifier l'objectif de chaque intervenant dans l'organisation du support. Elle est aussi importante pour déterminer si la réponse demandée a été fournie. Toutefois dans cet appel, consultants et ingénieurs supports ont travaillé en collaboration jusqu'à la fin de celui-ci afin de mettre en place une configuration cible permettant l'utilisation optimale de l'infrastructure.

L'implication des consultants, pourtant non systématique, était donc indispensable, étant donné que le projet venait d'être réalisé et que seuls les consultants pouvaient confirmer ce qui avait été vu ou configuré lors des phases de tests. Au vue de la gestion de l'appel et de l'implication d'HP, il était donc préférable de faire collaborer tous les intervenants pour bien comprendre l'impact de cet appel et définir le critère de résolution.

6. Actions correctives

6.1. Conventions.

Les principales informations techniques me permettant d'analyser un problème précis sont fournies par la récupération des logs sur les équipements. Un log est un fichier généré par un opérateur entrant des commandes spécifiques sur l'équipement désiré. Dans le cas de commutateurs MDS, il suffit d'entrer la commande "***show tech-support details***", qui génère automatiquement le résultat d'une centaine d'autres commandes, pour obtenir la génération des informations. Les logs des produits MDS sont très complets, comportant des sections par port, par process, mais aussi des logs détaillés sur l'historique des événements, des configurations, des modifications et également l'état des compteurs d'erreurs internes au commutateur. Au final, un fichier de plusieurs milliers de pages peut être généré; dans le cas traité, chaque commutateur générait un fichier d'environ 15000 pages. Il faut donc être capable de trier les informations utiles.
Dans les chapitres qui suivent les encadrés en vert correspondent à la partie des logs qui traite de la configuration. Les encadrés bleus, quant à eux, correspondent aux historiques des évènements ou au relevé des compteurs d'erreurs.
Afin de faciliter la lecture et la compréhension du mémoire, les relevés des logs et les analyses seront faits principalement depuis un seul commutateur (appelé Com-B2), l'approche, le comportement et les informations relevés dans les logs des autres commutateurs étant similaires.

6.2. Définition du problème principal

Le problème principal était une diminution des performances qui engendrait une incapacité à exécuter et à finir les copies sur les sites DR. Il fallait trouver la cause de ce défaut. Une analyse en profondeur des logs des commutateurs laissait entrevoir certains dysfonctionnements. La bonne utilisation de ces logs, associée aux informations sur le problème et l'infrastructure du client, permettent de bien s'imprégner de la configuration et d'être plus efficace lors de l'analyse et la création des plans d'actions. Le diagramme qui suit représente le cheminement que j'adopte généralement quand je travaille sur l'analyse technique d'un appel.
Ainsi, le travail peut se décomposer en trois phases principales. La première consiste en la création d'un schéma de la topologie afin de bien comprendre la configuration spécifique du client.
La seconde phase permet de faire une analyse précise et détaillée du problème, en analysant les sections qui permettent d'écarter immédiatement certaines causes puis en se concentrant sur les sections pouvant être en relation avec l'appel.
Enfin, la dernière phase reprend la mise en place des actions. En effet, une fois l'analyse avancée terminée il est possible de décrire les étapes suivantes, qui peuvent être des actions correctives ou des demandes d'informations supplémentaires. Cette partie comprend aussi l'élévation à l'équipe d'ingénierie si le problème ne peut pas être résolu à mon niveau. Cette équipe peut aussi être impliquée en cas d'escalade importante ou pour confirmer le travail et l'analyse déjà fournis au client. Il n'en reste pas moins que je suis le responsable de la réponse technique vers le support N1 ou le client et qu'il faut donc travailler en étroite collaboration avec l'ingénierie pour pouvoir être force de proposition.

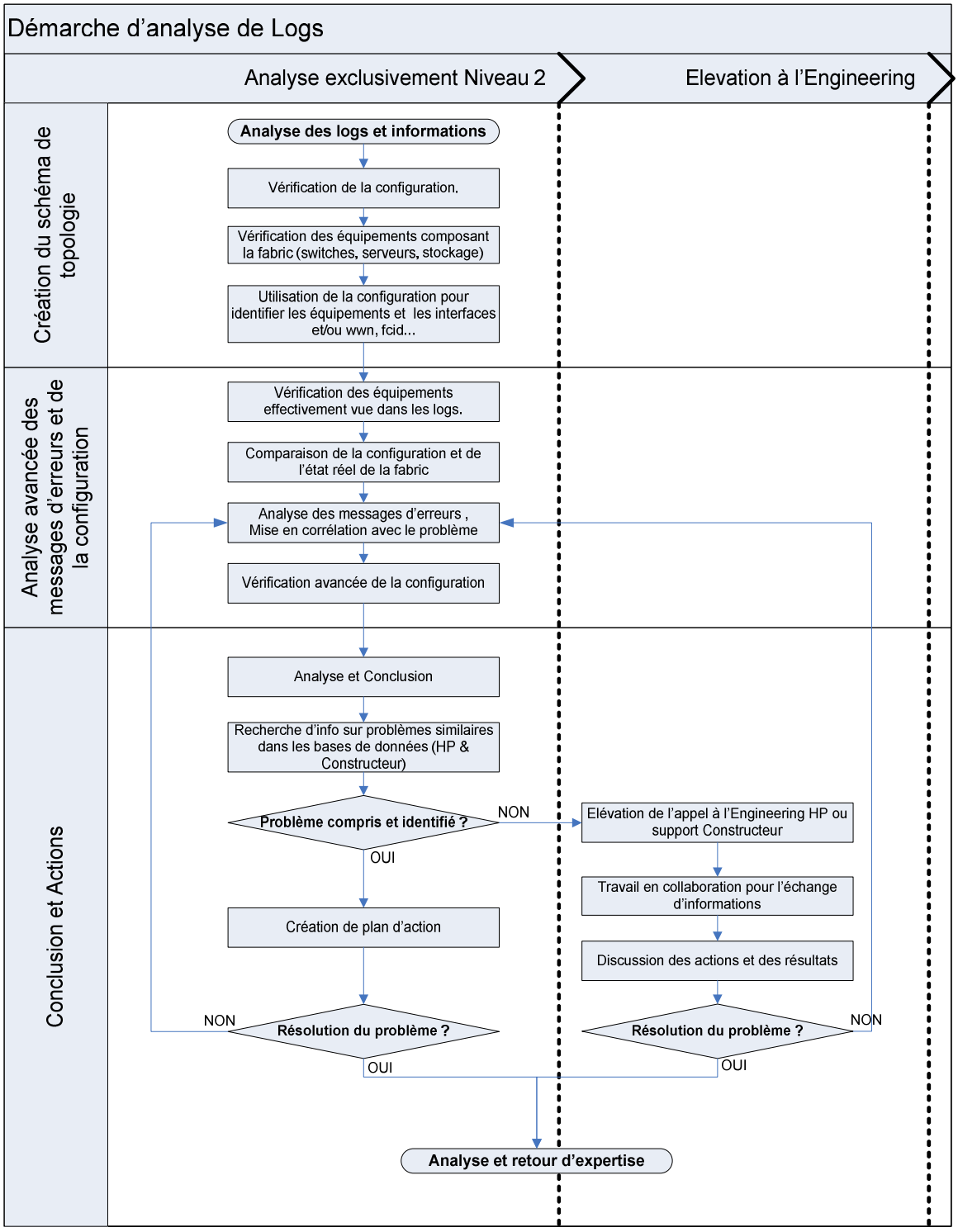


Figure 5: Démarche de l'analyse des logs.

Comme précisé dans le diagramme ci-dessus, j'ai l'habitude, quand je travaille sur un appel, de créer, dans un premier temps, un schéma de l'infrastructure. Ce graphique permet, par la suite, de bien distinguer les points sensibles ou de confirmer la stabilité d'autres points. Plus ce document est précis, plus il est facile de se repérer dans la fabric et donc de ne pas se perdre dans l'analyse des ports ou points non importants. Pour cet appel, j'ai réalisé les schémas suivants:

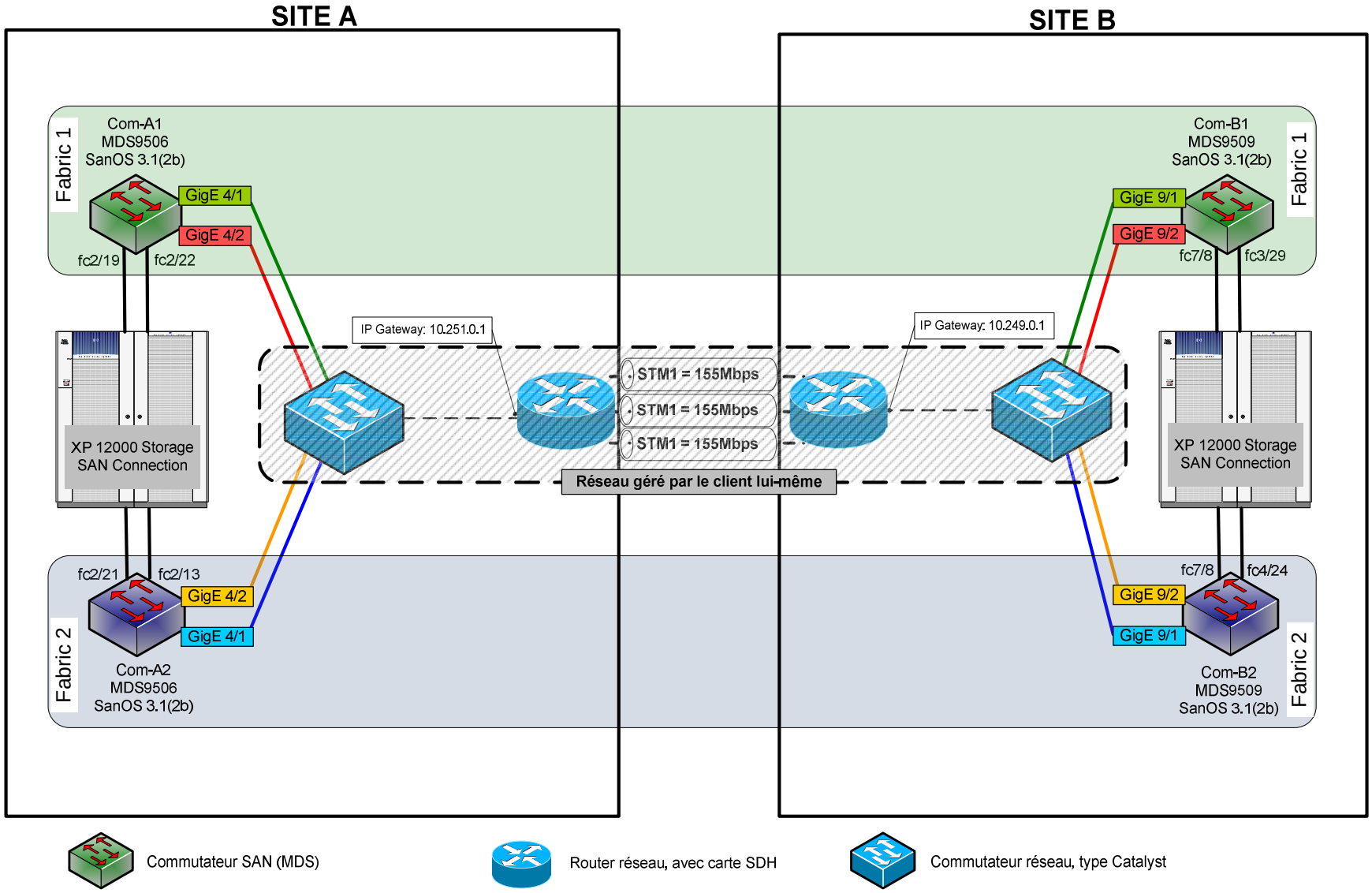


Figure 6: Schéma de l'infrastructure (couche physique) à l'ouverture de l'appel.

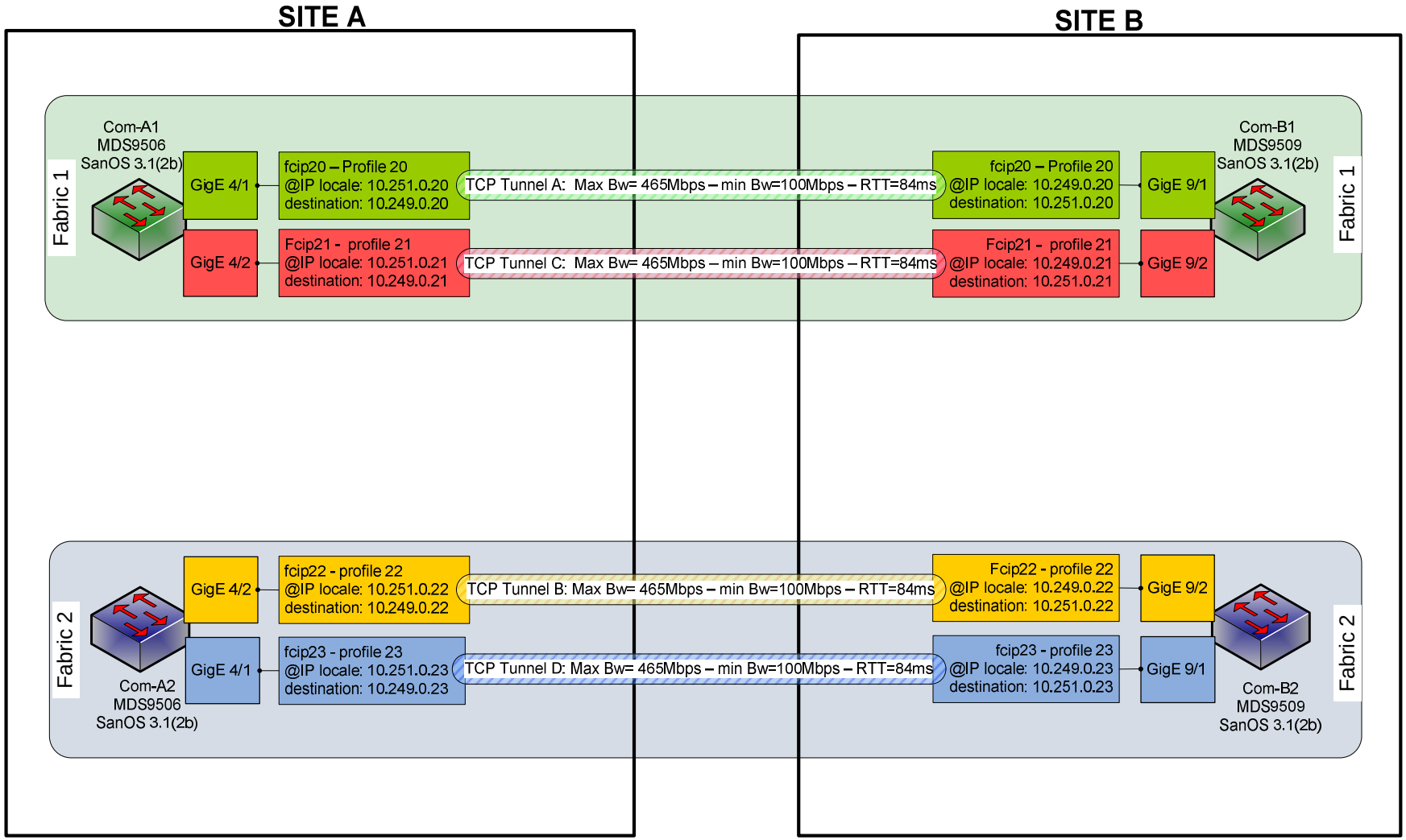


Figure 7: Schéma de l'infrastructure (couche logique) à l'ouverture de l'appel.

Une fois imprégné de la configuration du client, connaissant le problème global, il m'était donc possible de parcourir les logs une première fois, dans une approche assez large, afin de vérifier notamment si la configuration des commutateurs était conforme à l'infrastructure mais aussi aux règles de configuration. Cette section des logs est issue du "***show running-config***".

Certains points de configurations sont essentiels pour les commutateurs, suivant les fonctionnalités que l'on veut utiliser, que ce soit des fonctionnalités des commutateurs eux-mêmes ou sur les équipements connectés (baies de stockage,…). Dans le cas présent, les fonctionnalités principales étaient FCIP pour la partie commutateurs et CA[11] pour la partie baie de stockage.

► Confirmation de la version de microcode:

```
`show running-config`
version 3.1(2b)
```

Figure 8: Vérification de la version.

La version permet de confirmer que le microcode installé sur les commutateurs est bien connue comme stable et bien supportée par HP. Lors de l'appel la version du client n'était pas la plus récente, mais elle était toujours supportée et correspondait au dernier palier majeur, version SanOS 3.x. Ainsi elle était confirmée comme compatible avec les autres équipements installés.

► Vérification de la configuration des interfaces Gigabit Ethernet et du routage statique:

```
interface GigabitEthernet9/1
  ip address 10.249.0.23 255.255.255.0
  no shutdown

interface GigabitEthernet9/2
  ip address 10.249.0.22 255.255.255.0
  no shutdown

ip route 10.251.0.0 255.255.255.0 10.249.0.1
```

Figure 9: Vérification de la configuration des interfaces GigE - partie 1.

Les deux interfaces GigE[12] (9/1 et 9/2) sont bien configurées pour communiquer avec le réseau 10.251.0.0/24. A l'autre extrémité de la communication FCIP, le commutateur voisin sur l'autre site a bien ses deux interfaces GigE configurées de façon symétrique:

[11] CA : Continous Access, technologie HP pour permettre les copies directement entre les baies de stockage
[12] GigE : Gigabit Ethernet

```
(extrait de la configuration du commutateur distant Com-A2)

interface GigabitEthernet4/1
  ip address 10.251.0.23 255.255.255.0
  no shutdown

interface GigabitEthernet4/2
  ip address 10.251.0.22 255.255.255.0
  no shutdown

ip route 10.249.0.0 255.255.255.0 10.251.0.1
```

Figure 10: Vérification de la configuration des interfaces GigE - partie2.

Ainsi, d'après ces premières lignes de configurations, la partie IP de la configuration FCIP était correcte. La partie suivante va reprendre la configuration de l'encapsulation FC sur l'IP.

► Configuration de l'encapsulation FC sur IP:

Il faut activer la fonctionnalité FCIP et avoir la licence associée. Puis, une fois la commande "***fcip enable***" entrée, il faut configurer les profils FCIP. Ces profils permettent d'établir la configuration du tunnel TCP qui supportera la communication FCIP inter-commutateurs.

```
fcip enable

fcip profile 22
  ip address 10.249.0.22
  tcp max-bandwidth-mbps 465 min-available-bandwidth-mbps 100  round-trip-time-ms 84

fcip profile 23
  ip address 10.249.0.23
  tcp max-bandwidth-mbps 465 min-available-bandwidth-mbps 100  round-trip-time-ms 84
```

Figure 11: Vérification de la configuration des profils FCIP.

Il est possible de constater que les profils 22 et 23 sont bien associés avec les adresses IP des interfaces GigE 9/2 et 9/1 respectivement. Aussi, les paramètres TCP Max/min sont configurés pour 2x 465 Mbps pour une bande passante maximum et 2x100 Mbps pour le seuil minimum. Le RTT [13]est configuré à 84 ms. Ces trois valeurs feront l'objet d'analyses plus complètes un peu plus loin lors du dépannage plus avancé.

Les autres paramètres n'étant pas indiqués dans la section "show running-config", cela signifie que les valeurs par défaut sont utilisées. A ce stade de l'analyse, je ne peux pas savoir si les valeurs, même par défaut, sont pertinentes avec les besoins et les caractéristiques de l'infrastructure, mais, dans la plupart des installations, la configuration mise en place est cohérente et ne montre pas de manquement grave pouvant perturber la fabric.

► Configuration des interfaces FCIP:

La configuration des interfaces FCIP permet d'activer ou non, différentes options que l'on veut utiliser. Ces options sont principalement liées à des optimisations au niveau du trafic FC. Elles peuvent être : agrégation de liens intersites (portChannel), compression du trafic (ip-

[13] RTT : Round Trip Time, est le temps que met un paquet à aller et revenir d'un point à l'autre de la connexion TCP.

compression), accélération des échanges de messages lors de la communication entre les équipements (write ou tape accelerator). Ces paramètres sont donc configurés dans la configuration des interfaces FCIP.

```
interface fcip22
  channel-group 1 force
  use-profile 22
  peer-info ipaddr 10.251.0.22
  write-accelerator
  ip-compression mode1
  no shutdown

interface fcip23
  channel-group 1 force
  use-profile 23
  peer-info ipaddr 10.251.0.23
  write-accelerator
  ip-compression mode1
  no shutdown
```

Figure 12: Vérification de la configuration des interfaces FCIP.

De la même façon, il faut contrôler les configurations à chaque extrémité, afin de s'assurer de la cohérence des informations entrées. Il faut, en effet, faire correspondre les interfaces entre-elles, en utilisant le paramètre "peer-info" dans l'interface FCIP adéquat, et activer les mêmes fonctionnalités à chaque extrémité.

Dans l'encadré ci-dessus, on observe principalement 3 éléments importants:

1- L'utilisation du port Channel [14] (channel-group) qui permet l'agrégation des interfaces FCIP22 et 23, puisqu'ils ont le même indice "1" de port-channel.

2- L'utilisation de l'accélération en écriture (write-accelerator)

3- La compression de mode 1, associée à l'utilisation du module 8 ports GigE, qui optimise la compression pour des liens avec une bande passante supérieure à 25Mbps.

Les trois points identifiés sont très importants pour la stabilité du trafic. Car, s'ils permettent d'améliorer les performances, ils peuvent, dès lors que leur utilisation n'est pas adaptée, engendrer des baisses de performances très importantes. Ainsi, ces trois fonctionnalités et la configuration TCP max et min de la bande passante vont être les premiers points identifiés comme potentiellement problématiques.

A ce stade de l'analyse, je sais quels points il faudra analyser en détails, en priorité afin de s'assurer que les commutateurs sont dans la configuration requise pour fournir le service prévu. Et en même temps, il m'est possible de commencer à lister les premiers points du plan d'actions que j'aurai à fournir. Ce plan d'actions peut faire partie intégrante du rapport d'escalade, qui est le document officiel résumant les actions menées.
Ce rapport est en Annexe 1, page 71.

Les plans d'actions sont les tâches les plus importantes au niveau du support. En effet, ils servent de guide lors des étapes suivantes du dépannage. Ils incluent la commande de matériels, le déplacement d'ingénieurs spécialisés sur site pour assister le client dans le dépannage,… De plus, c'est par ces plans d'actions que j'ai démontré au client ma maîtrise et

[14] Le « port-channel » est l'agrégation de plusieurs liens physiques en un seul lien logique.

ma compréhension de son problème et aussi, la pertinence de mes propositions et de mon analyse. D'une manière générale, il faut qu'ils soient cohérents, précis avec des tâches bien définies, réalistes. Ils doivent prendre en compte les impératifs de productions du client.

6.3. Stabilisation

Afin d'exploiter au mieux les messages d'erreurs et les compteurs d'événements, il faut pouvoir confirmer si les informations sont liées à la cause ou à une conséquence du problème. Ainsi, il est parfois très difficile, voire impossible, d'exploiter ces informations si l'environnement n'est pas stable (coupure de liaison directe,…). Les premières actions à fournir doivent permettre une stabilisation de l'infrastructure afin de pouvoir par la suite interpréter au mieux les messages et les incrémentations de compteurs d'erreurs persistants.

La seconde phase de mon analyse est orientée sur les messages d'erreurs et les relevés des compteurs (trafic, erreur, initialisation,…). La première section à laquelle je m'intéresse est donc celle qui enregistre tous les messages d'erreurs, incluant la date, l'heure et les détails sur l'erreur elle-même. Ainsi, connaissant l'historique du problème, je peux à présent constater dans les événements des commutateurs si certains messages d'erreurs ont bien été enregistrés. Cette section des logs est issue du "***show logging log***"

```
2008 Mar 18 04:56:27 Com-A2 %PORT-5-IF_DOWN_TCP_MAX_RETRANSMIT: %$VSAN 1%$ Interface
fcip23 is down(TCP conn. closed - retransmit failure)

2008 Mar 18 04:56:27 Com-A2 %PORT-5-IF_DOWN_TCP_MAX_RETRANSMIT: %$VSAN 1%$ Interface
fcip22 is down(TCP conn. closed - retransmit failure)

…/…

2008 Mar 18 04:58:01 Com-A2 %PORT-5-IF_TRUNK_UP: %$VSAN 1%$ Interface fcip23, vsan 1 is up
2008 Mar 18 04:58:01 Com-A2 %PORT-5-IF_TRUNK_UP: %$VSAN 1%$ Interface fcip22, vsan 1 is up
```

Figure 13: Show logging log - Partie 1.

Dans cette section du commutateur Com-A2, il est possible de voir que les tunnels TCP se sont fermés car il y a eu trop de retransmissions. Par défaut, il y a 4 tentatives de retransmissions. Du point de vue de ce commutateur, il n'y a pas beaucoup plus d'explications. Il est possible que ces retransmissions soient dues à des erreurs physiques sur la ligne ne permettant pas une transmission de qualité suffisante pour reconnaître les trames de services. Il est possible aussi qu'un opérateur ait interrompu volontairement la liaison… Afin de comprendre les raisons de cette coupure, il faut donc analyser les messages du commutateur opposé.

```
2008 Mar 18 04:35:46 Com-B2 %ETHPORT-5-IF_DOWN_SOFTWARE_FAILURE: Interface
GigabitEthernet9/1 is down (Port software failure)

2008 Mar 18 04:35:46 Com-B2 %ETHPORT-5-IF_DOWN_SOFTWARE_FAILURE: Interface
GigabitEthernet9/2 is down (Port software failure)

…/…

2008 Mar 18 04:36:03 Com-B2 %IPS_SB_MGR-SLOT9-2-PORT_SOFTWARE_FAILURE: Port software
failure, module 9 port 1

2008 Mar 18 04:36:03 Com-B2 %IPS_SB_MGR-SLOT9-2-PORT_SOFTWARE_FAILURE: Port software
failure, module 9 port 2

…/…

2008 Mar 18 04:36:12 Com-B2 %ETHPORT-5-IF_UP: Interface GigabitEthernet9/1 is up
2008 Mar 18 04:36:12 Com-B2 %ETHPORT-5-IF_UP: Interface GigabitEthernet9/2 is up

…/…

2008 Mar 18 04:36:31 Com-B2 %PORT-5-IF_TRUNK_UP: %$VSAN 1%$ Interface fcip23, vsan 1 is up
2008 Mar 18 04:36:31 Com-B2 %PORT-5-IF_TRUNK_UP: %$VSAN 1%$ Interface fcip22, vsan 1 is up
```

Figure 14: Show logging log - Partie 2.

Dans le commutateur Com-B2, il est possible de voir que les ports GigE sont passés "down". Ceci signifie que les interfaces associées sont donc aussi "down". (Interfaces FCIP, portchannel,…) et que les tunnels TCP sont donc aussi stoppés, comme on le voit effectivement sur le commutateur Com-A2. De ce fait, aucun trafic IP et a fortiori FC ne peut passer entre les commutateurs. Dans cet état on dit que la fabric est segmentée[15]. Il semble donc que l'initiateur de la déconnexion soit Com-B2.

On s'aperçoit aussi de deux informations essentielles. La première est que l'événement qui a coupé les interfaces GigE semble être dû à une défaillance logicielle. La seconde est que les ports se sont remis à fonctionner automatiquement seulement quelques secondes après la défaillance. Ce type d'empreinte laisse présager un problème au niveau logiciel sur le commutateur. Dans les étapes du plan d'actions, il m'est donc possible d'ajouter une tâche liée à la vérification de la version logicielle et de son comportement dans ce type de configuration avancée.

Dans tous les cas, un défaut de ce type va entraîner une très forte perturbation sur le trafic et donc une diminution très forte de performance. D'autant plus, qu'il m'était possible de voir ce type d'événements plusieurs fois sur les quatre commutateurs. De part cette première analyse, il m'est donc possible de pointer un incident compatible avec le comportement vu sur site.

Après une recherche dans les release notes[16] des versions logicielles postérieures à celle utilisée par le client, je me suis aperçu qu'il y avait un bug correspondant à la configuration du client et à la perturbation du tunnel TCP. Cette anomalie logicielle était identifiée de la manière suivante dans la release note:

[15] La segmentation signifie que la liaison entre 2 commutateurs est interrompue. Cela peut être dû à un problème de communication (erreur physique, logicielle,…) ou une incompatibilité des paramètres créant ainsi une incapacité à communiquer et a autoriser les commutateurs à échanger du trafic FC.

[16] Les Release Notes, sont les documents officiels constructeurs informant des nouveautés, modifications, corrections de défauts apportés dans la version logicielle spécifiée.

-FCIP link may fail with WA/TA turned on
-DMA bridge shows iscsi crc err

Symptom: *FCIP links running Write Acceleration/Tape Acceleration with Compression set to mode 1 may fail intermittently for no apparent reason.*

Conditions: *Unknown at this time.*

Workaround: *Disable FCIP WA/TA.*

1st Found-In: *3.1(2b)*

Fixed-In: *3.2(0.109)*

Information issue de la release note Cisco du SanOS 3.2

En faisant l'analogie entre le descriptif du bug et la configuration des commutateurs, il est possible de constater que la version logicielle du client correspondait, SanOS 3.1(2b), la compression Mode1 était activée et la fonctionnalité de Write-Acceleration (WA) l'était aussi. L'instabilité des interfaces FCIP et du tunnel TCP correspondait bien au problème rencontré sur site. Donc, à cette étape, il était clairement établi que le plan d'actions comporterait des actions visant à fixer ce défaut. Maintenant, il me revenait d'établir les actions à mener:

► Etait-il mieux de mettre à jour la version immédiatement ?

►Fallait-il stopper les fonctionnalités ? (comme indiqué dans le workaround[17])

Les deux options, qu'il m'était possible de mettre en œuvre, présentaient chacune un inconvénient important. Pour la première, dans une situation très complexe avec beaucoup de tension entre le client et le fournisseur de service (HP Support), était-il réellement préférable de conseiller une mise à jour logicielle de grande ampleur, en sachant pertinemment que l'infrastructure, même si elle serait stabilisée, ne serait pas totalement corrigée ? Ceci d'autant plus que la mise à jour des commutateurs allait engendrer la mise à jour des logiciels et applications des serveurs, de leurs périphériques (cartes HBA[18], …) et des baies de stockage. Néanmoins, cette solution présentait l'intérêt de ne pas supprimer volontairement les optimisations (pour améliorer les performances) qui étaient déjà réduites. Sur ce point, la seconde option était donc très délicate à présenter. Non seulement les performances n'étaient déjà pas bonnes, mais la suppression de ces fonctionnalités allait probablement les diminuer encore plus.
Finalement, c'est la seconde action que j'ai choisi de présenter comme première étape dans la stabilisation de l'infrastructure. Ce choix me permettait de couvrir plusieurs aspects. Premièrement, il n'était pas certain que la configuration de la compression et de l'accélération soient faites de façon pertinente par rapport au type de trafic et à la bande passante. Ainsi, la suppression de ces options allait permettre de continuer le dépannage avec une configuration plus basique. Deuxièmement, il était quasi certain que les instabilités rencontrées sur la partie IP allaient disparaître immédiatement, ce qui permettait une stabilisation bien plus rapide,

[17] Workaround : est une solution de contournement afin de ne pas rentrer dans le périmetre du bug.
[18] HBA : Host Bus Adaptor. Carte présente dans le serveur comportant les éléments (Asic, connecteurs, …) pour la connexion aux équipements extérieurs (commutateurs, baie de stockage)

faisant gagner du temps pour la suite des opérations. Enfin, et même si ce point est assez peu en relation avec la technique, le fait de ne pas proposer un upgrade permettrait certainement de rassurer le client sur l'approche que j'avais. En effet, si on se met à la place d'un client, il est désagréable de s'entendre dire "faites un upgrade, puis ensuite on verra…". Même si la proposition de mise à jour pouvait être justifiée, proposer autre chose qu'un upgrade renforçait la conviction que le problème était bien compris et que le diagnostic associé correspondait aux besoins du client. Naturellement, cette option a rencontré des réticences, car il y avait un risque de réduire encore un peu plus les performances. Mais mon argumentation a permis de valider cette opération. Il a donc été décidé de modifier la configuration des commutateurs en stoppant les fonctions de compression et d'accélération.

Néanmoins, même si ce défaut était clairement pointé comme la raison potentielle du problème, il ne pouvait être le seul responsable. En effet, les problèmes de performances apparaissaient même si les tunnels TCP et interface FCIP, GigE semblaient fonctionner normalement.

Un autre point avait attiré mon attention très tôt dans l'analyse de la configuration. Le paramétrage de la bande passante maximum n'était pas bon. Lors de la configuration des profils FCIP, on doit entrer la valeur de la bande passante maximale disponible pour chaque connexion TCP. Dans le cas présent, il y avait deux interfaces FCIP sur chaque commutateur. Il y avait deux commutateurs par sites. Donc, il y avait quatre tunnels TCP actifs simultanément qui se partageaient la bande passante totale allouée au trafic FCIP. Au début de mon analyse, le client confirmait bien qu'il y a avait 3 liens à 155 Mbps (soit au total 465 Mbps) disponibles pour le trafic intersites. Toutefois, je lui ai demandé de me confirmer sur ces 465 Mbps, quelle était la bande passante effectivement dédiée au trafic de réplication. En fait, la réponse était différente, et en réalité, la bande passante pour le trafic de réplication était de 410 Mbps, répartie sur 2 tunnels STM1 (155 Mbps chacun) et le troisième tunnel STM1 partagé pour 55 Mbps de trafic IP divers et 100 Mbps de trafic dédié à la réplication. Comme 4 tunnels TCP se partageaient cette bande passante de 410 Mbps, il fallait la diviser par quatre. Le résultat nous donnait donc une bande passante maximum par tunnel TCP de 102,5 Mbps que j'ai arrondie à 100 Mbps. La valeur minimum, quant à elle, est liée au comportement TCP lors de retransmission, je l'ai ajustée à 80% de la valeur maximum (comme la documentation constructeur le conseille). Le fournisseur réseau confirmait que le RTT était bien de 84 ms. De ce fait, je proposais une deuxième action nécessitant la reconfiguration de la bande passante pour les tunnels TCP. Cette opération a donc été faite en même temps que la suppression des fonctions de compression et d'accélération. Il est très important de bien configurer ces paramètres TCP car, autrement, il y a de forts risques de retransmissions et donc les performances peuvent être fortement dégradées. Ce point était aussi une action majeure dans l'établissement de mon plan d'actions.

Les commandes associées sont les suivantes:

```
Com-B2# config terminal

Com-B2(config)# fcip profile 22
Com-B2(config-profile)# tcp max-bandwidth-mbps 100 min-available-bandwidth-mbps 80  round-
trip-time-ms 84
Com-B2(config-profile)#exit
Com-B2(config)# interface fcip 22
Com-B2(config-if)# no write-accelerator
Com-B2(config-if)# no ip-compression mode1
Com-B2(config-if)# exit
Com-B2(config)# exit

Com-B2(config)# fcip profile 23
Com-B2(config-profile)# tcp max-bandwidth-mbps 100 min-available-bandwidth-mbps 80  round-
trip-time-ms 84
Com-B2(config-profile)#exit
Com-B2(config)# interface fcip 23
Com-B2(config-if)# no write-accelerator
Com-B2(config-if)# no ip-compression mode1
Com-B2(config-if)# exit
Com-B2(config)# exit

Com-B2# copy running-config  startup-config
[########################################] 100%
Com-B2#
```

Figure 15: Configuration lors de la stabilisation.

En utilisant des outils internes HP de connexions à distance, j'ai pu prendre la main sur les équipements du client et entrer les nouvelles valeurs. Avant de faire la modification de la configuration, j'avais pris soin de tester sur une plate-forme les commandes que j'allais passer dans la nuit. J'allais devoir intervenir sur une infrastructure de production et il était inconcevable que je puisse faire une quelconque erreur lors de cette phase de mon plan d'actions.
Lors de la modification des paramètres TCP d'un profile FCIP, le tunnel se ferme automatiquement dès lors que les paramètres à chaque extrémité ne sont pas identiques. Ce qui signifie que l'interface FCIP associée serait "down" le temps de faire la reconfiguration du côté opposé. Ce temps d'indisponibilité était de quelques secondes. Ainsi, j'ai appliqué la modification lien par lien, en attendant à chaque fois que l'interface soit remontée avec le nouveau paramétrage avant de modifier l'interface suivante. Ceci afin d'éviter une segmentation de la fabric, qui aurait eu un impact très grave sur l'appréciation de mon travail auprès du client.

Enfin, une fois ce travail accompli, puis après une nuit d'observation, il a été possible de confirmer que les tunnels TCP étaient redevenus stables. Nous étions donc capables de continuer l'analyse et le dépannage dans un environnement stabilisé. De plus, l'hypothèse de retransmission due à la saturation du lien, provenant de la mauvaise configuration de la bande passant maximum par tunnel TCP était aussi supprimée. Ainsi, l'état des compteurs, suite à l'application des actions précédentes, pouvait être pleinement pris en compte dans la suite des actions à mener.

6.4. Fausses pistes

Lors de l'établissement d'un plan d'actions, peu ou pas de pistes sont écartées dans la première approche. Puis suivant le résultat des actions, des tests ou des logs, il est possible de réajuster le plan d'actions afin qu'il soit plus cohérent avec l'état actuel des recherches et de l'avancée du problème. Néanmoins, il existe parfois des conditions qui font que le travail s'oriente sur des fausses pistes sans qu'il soit réellement possible de s'en rendre compte immédiatement. En

effet, très souvent ces fausses pistes sont confirmées comme telles une fois que leur diagnostic est terminé. Cela peut entraîner parfois une perte de temps, des actions inutiles et dans les cas les plus gênant un certain découragement des personnels impliqués, surtout lors d'appels critiques demandant un investissement important.

Dans le cas présent, même si nous avons dû travailler sur des fausses pistes, les investigations non pas été veines, car elles ont permis de réduire les possibilités du défaut, en d'autres termes, ont permis de confirmer certains points de stabilité. En même temps, il a été possible de mettre en avant des comportements qui n'étaient pas la source du problème, mais ses conséquences. Ces deux aspects me servent aujourd'hui dans mon travail au quotidien.

6.4.1. Baies de stockage XP et Buffer credit

Avant d'avoir une liaison FCIP opérationnelle, il était très difficile de différencier les événements et de savoir ce qui résultait d'une conséquence de l'instabilité ou non. Ainsi, une fois la connexion TCP stable, il était donc possible de se concentrer sur les autres événements. J'ai pu ensuite confirmer que certaines connexions aux ports de la baie de stockage (Baie XP) présentaient une incrémentation importante au niveau des compteurs d'erreurs. Ces erreurs étaient pour l'essentiel des déconnexions/reconnexions intempestives, de très courtes durées, principalement sur le port fc4/24 du commutateur Com-B2.

L'équipe locale avait déjà travaillé sur ce problème, mais sans l'analyser complètement. Ils avaient donc déjà changé plusieurs composants et même déplacé la connexion depuis l'interface fc3/25 vers la fc4/24. Puisque le problème était revenu, il me demandait donc d'analyser ce problème qui pouvait aussi être la source d'un souci de performance, puisque les déconnexions touchaient les ports de baies de stockage.

Pour bien repérer ce problème il m'a fallu vérifier toutes les connexions aux ports de baies de stockage puis après avoir sélectionné l'interface fc4/24 du commutateur Com-B2, il fallait analyser deux sections dans les logs du commutateur:

► 1ère étape, faire un delta entre deux collections de logs:

-collection 1: `Thu Mar 20 09:49:46 EET 2008`

```
3171104 frames input, 6517829100 bytes
  0 discards, 3 errors
  0 CRC,  0 unknown class
  0 too long, 0 too short
49824 frames output, 25050452 bytes
  0 discards, 0 errors
29 input OLS, 29 LRR, 0 NOS, 49 loop inits
46 output OLS, 111 LRR, 43 NOS, 49 loop inits
```

Figure 16: Analyse des compteurs d'erreurs FC - Collection 1.

-collection 2: Fri Mar 21 03:49:44 EET 2008

```
      10019353 frames input, 20617439080 bytes
        0 discards, 3 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      85637 frames output, 5632156 bytes
        17 discards, 0 errors
      1732 input OLS, 1690 LRR, 0 NOS, 169 loop inits
      1089 output OLS, 1026 LRR, 1083 NOS, 191 loop inits
```

Figure 17: Analyse des compteurs d'erreurs FC - Collection 2.

Il est possible d'analyser entre les deux collections que l'interface a eu un nombre important d'événements liés à des resynchronisations de la liaison FC. Ces événements sont enregistrés par les compteurs OLS, LRR, NOS, qui sont des messages de transmission (appelés "primitive Sequence") définis par protocole Fibre Channel.

---

*Primitive Sequences are transmitted to indicate specific conditions within or conditions encountered by the receiver logic of an FC_Port. Primitive Sequences shall be transmitted continuously while the condition exists. The **NOS**, **OLS**, **LR**, and **LRR** Primitive Sequences shall be supported.*

***NOS**: Non Operational Sequence : The NOS Primitive Sequence shall be transmitted to indicate that the FC_Port transmitting the NOS has detected a Link Failure condition or is Offline, waiting for OLS to be received.*

***OLS**: Offline Link Sequence : The OLS Primitive Sequence shall be transmitted to indicate that the FC_Port transmitting the Sequence is initiating the Link Initialization Protocol, receiving and recognizing NOS and entering the Offline State.*

***LR**: Link Reset: The LR Primitive Sequence shall be transmitted by an FC_Port to initiate the Link Reset Protocol or to recover from a Link Timeout.*

***LRR**: Link Reset Response: The LRR Primitive Sequence shall be transmitted by an FC_Port to indicate that it is receiving and recognizes the LR Primitive Sequence.*

Informations issues du document FC-FS de l'ANSI.

L'incrémentation importante de ces compteurs m'indiquait clairement que la connexion entre le commutateur et la baie de stockage était instable. Ces instabilités n'étaient pas dues à une mauvaise connexion physique car, les compteurs de CRC (entre autres) se seraient incrémentés eux aussi. Le log suivant me permettait d'en connaître un peu plus sur les raisons de ces instabilités.

```
module-4# show port internal link-events
*************** Port Config Link Events Log ***************
----                            ------  -----  -----  ------
Time                            PortNo  Speed  Event  Reason
----                            ------  -----  -----  ------
Mar 21 03:50:12 2008  00197272  fc4/24   2G     UP    Not FL
Mar 21 03:50:12 2008  00095400  fc4/24   ---   DOWN   LR Rcvd B2B
Mar 21 03:49:57 2008  00225688  fc4/24   2G     UP    Not FL
Mar 21 03:49:57 2008  00124480  fc4/24   ---   DOWN   LR Rcvd B2B
Mar 21 03:49:43 2008  00825899  fc4/24   2G     UP    Not FL
Mar 21 03:49:43 2008  00635593  fc4/24   ---   DOWN   LR Rcvd B2B
Mar 21 03:49:29 2008  00957000  fc4/24   2G     UP    Not FL
Mar 21 03:49:29 2008  00870708  fc4/24   ---   DOWN   LR Rcvd B2B
Mar 21 03:49:16 2008  00734163  fc4/24   2G     UP    Not FL
Mar 21 03:49:16 2008  00637096  fc4/24   ---   DOWN   LR Rcvd B2B
Mar 21 03:49:03 2008  00206510  fc4/24   2G     UP    Not FL
Mar 21 03:49:03 2008  00021068  fc4/24   ---   DOWN   LR Rcvd B2B
Mar 21 03:48:49 2008  00846018  fc4/24   2G     UP    Not FL
Mar 21 03:48:49 2008  00760562  fc4/24   ---   DOWN   LR Rcvd B2B
Mar 21 03:48:36 2008  00045324  fc4/24   2G     UP    Not FL
Mar 21 03:48:35 2008  00953663  fc4/24   ---   DOWN   LR Rcvd B2B
Mar 21 03:48:22 2008  00665210  fc4/24   2G     UP    Not FL
Mar 21 03:48:22 2008  00577414  fc4/24   ---   DOWN   LR Rcvd B2B
```

Figure 18: Erreur explicitant l'instabilité des ports de baies.

Ainsi, il était possible de voir que l'interface fc4/24 passait constamment en UP/DOWN sur des périodes extrêmement courtes (L'indicateur de temps montre que la durée entre le moment où l'interface passe "DOWN" et celui où elle est "UP" est inférieur à la seconde). De plus, la durée moyenne entre deux événements est d'environ 13 secondes, il s'agissait donc d'un problème récurrent avec une fréquence stable apparaissant en rafales plus ou moins longues. La raison associée était "LR Rcvd B2B[19]"("Link Reset Received Buffer to Buffer"). La traduction de ce message est que l'interface du commutateur recevait des commandes de réinitialisation pour des problèmes de disponibilité de mémoires tampons. En fait, à chaque fois qu'une trame est envoyée, elle transite par une mémoire tampon (un "buffer") avant d'être traitée, en interne, par le commutateur ou envoyée sur la fibre. Ce traitement peut être plus ou moins long suivant l'occupation mémoire, suivant l'occupation processeur du commutateur, suivant la distance, ou suivant la saturation de ligne,…. Ainsi, ce processus permet de contrôler la transmission des trames afin de ne pas engorger le réseau.
Il existe un mécanisme qui autorise l'interface transmetteur à envoyer une nouvelle trame, quand l'interface réceptrice a un nouveau buffer disponible. Ce mécanisme utilise le message de contrôle "R_RDY[20]", spécifié par le protocole FC. A chaque fois qu'un nouveau buffer est disponible, autrement dit, à chaque fois que le récepteur a transmis en interne au commutateur une nouvelle trame pour être traitée, il émet au transmetteur le message R_RDY. Ainsi, le transmetteur sait qu'il peut envoyer une nouvelle trame et que le récepteur est prêt à la prendre en charge. Toutefois, il peut arriver que le récepteur n'envoie pas de R_RDY (par exemple si le commutateur est fortement occupé par d'autres opérations), dans ce cas, le transmetteur, après avoir atteint un timeout [21](E_D_TOV[22]), émet un signal Link Reset afin de réinitialiser les compteurs des buffers.

[19] B2B : Buffer to Buffer Credit, est l'acronyme utilise pour designer la mémoire tampon d'une interface FC.
[20] R_RDY : Receiver Ready, est le message de contrôle qui permet de prévenir le transmetteur que le récepteur a un nouveau buffer de disponible.
[21] Timeout : dépassement du temps imparti
[22] E_D_TOV : Error Detect TimeOut Value : Compteur utilisé pour détecter une erreur dans la durée de transmission de messages de contrôle. La valeur par défaut est 2000ms.

---

*A Link timeout error shall be detected if one or more **R_RDY** Primitive Signals are not received within **E_D_TOV** after the buffer-to-buffer Credit_CNT has reached zero.*
Recovery from Link timeout is accomplished by performing the Link Reset Protocol.

Informations issues du document FC-FS de l'ANSI.

C'était, en partie, le comportement qu'on constatait sur le commutateur et, dans ces conditions, il m'était donc possible de confirmer que ce défaut résultait plutôt du problème de performance. Puisque que le réseau était fortement ralenti, il se pouvait que certains ports puissent ne pas traiter les trames dans les temps impartis par le protocole. Toutefois, le Link Reset généré pour le rétablissement des buffers, ne doit pas forcer l'interface à l'état Down. Ainsi, pour ce problème spécifique, il devait y avoir une autre source de défaut, qui est habituellement liée à la partie physique (SFP, câbles,…). Pourtant, l'équipe locale avait déjà remplacé la majeure partie du matériel et aussi changé d'interface sur le module, il était donc quasi certain que le problème n'était pas lié à un composant défectueux.
Afin de pouvoir dépanner complètement ce défaut, il a donc fallu prendre des traces FC à l'aide d'un analyseur de protocole et contacter l'équipe d'ingénierie pour traiter ce problème spécifique séparément. Néanmoins, je confirmais tout de même à l'équipe locale qu'il n'y avait pas d'intérêt à changer d'autres pièces et, une fois le problème de performances résolu, ce défaut de déconnexion devrait disparaître.

6.4.2. Ping & QoS

Dans le monde du réseau, lorsqu'on veut vérifier rapidement la stabilité et la connectivité entre deux équipements, il est très courant d'utiliser la commande "ping". Cette commande est disponible aussi sur les commutateurs Fibre Channel du constructeur Cisco (Gamme MDS). Ainsi, il est possible de tester la liaison entre les deux interfaces GigE du site local vers le site distant. J'ai demandé aux équipes locales de le réaliser lors de notre travail de dépannage. Très rapidement, il a été possible de constater que les performances reportées n'étaient pas celles attendues.

Ci-dessous, le résultat de "ping" depuis le commutateur Com-B2 interface GigE9/2 vers Com-A2 interface GigE4/2.

```
--- 10.251.0.22 ping statistics ---
500 packets transmitted, 497 received, 0% packet loss, time 504019ms
rtt min/avg/max/mdev = 80.249/84.829/137.910/6.507 ms
```

Figure 19: Résultat de la commande "ping".

A travers ce résultat, il était possible, en ayant fait l'analyse sur une durée assez courte d'environ 8 minutes, de remarquer que le réseau ne répondait pas au "ping" de la façon voulue. En effet, sur 500 paquets émis, 3 paquets étaient perdus. De plus, la valeur du RTT, présentait tout de même des fluctuations importantes, allant jusqu'au maximum de 137 ms, bien que la moyenne soit effectivement de 84 ms, comme configurée dans les profiles FCIP. Ces valeurs, présentées de cette façon, ne semblent pas forcément incompatibles avec l'infrastructure. Mais, il faut savoir que, dès lors qu'on veut faire du "Continous Access", il est impératif d'avoir un réseau extrêmement stable. Ci-dessous, les spécifications demandées par l'ingénierie HP:

Average packet-loss ratio*(1): Low-loss network: 0.0012% average over 24 hours*
High-loss network: 0.2% average over 24 hours; must not exceed 0.5% for more than 5 minutes in a 2-hour window

Latency jitter*(2): Must not exceed 10 ms over 24 hours*

(1)A high packet-loss ratio indicates the need to retransmit data across the ISL. Each retransmission delays transmissions queued behind the current packet, thus increasing the time to complete pending transactions.
(2)Latency jitter is the difference between the minimum and maximum values, and indicates how stable or predictable the network delay is. The greater the jitter, the greater the variance in the delay, which lowers the performance predictability.

Informations issues du San Design Guide de HP

Si on estime comme dans le test des 500 ping, qu'il y a un ping à la seconde. Alors, un test de 24h donnera environ 86400 ping envoyés. Si le réseau était un réseau dit à "forte perte" alors, il y aurait 0,2% des 86400 paquets qui seraient perdus, ce qui donne approximativement 173 pertes. Avec 3 paquets perdus pour 500 ping, on aurait alors environ 518 pertes sur 24h. On voit donc que l'on dépasse largement les 173 pertes sur une durée de 24h. Pour ces raisons, si le problème de pertes de paquets était confirmé, il était fort probable que les problèmes de performances en résultaient directement et, qu'alors le problème se déplaçait sur le réseau du fournisseur de service et non plus sur les commutateurs ou baies de stockages.
Par manque de temps, ce test n'a pas pu être effectué sur une période de 24h. Mais, la discussion avec le fournisseur de service a tout de même été engagée, et il a travaillé, avec ses équipes, afin de vérifier pourquoi il y avait de si mauvaises statistiques sur le réseau.

J'avais pris la précaution de modérer nos propos envers ce problème potentiel de pertes de paquets, pour deux raisons principales. La première était que, même sur un réseau dédié à la réplication intersites, les équipements réseaux de type routeurs peuvent être configurés pour utiliser la QoS, celle-ci appliquant des règles de priorités différentes suivant le type de trafic. Il n'était donc pas improbable que le fournisseur de service ait marqué le trafic de réplication avec la plus haute priorité, rendant, par conséquent, d'autres types de trafic moins prioritaires. Les paquets de type "ping" sont des paquets ICMP[23], qui ne sont pas prioritaires sur le trafic de réplication et donc, si des règles de QoS avaient été mises en place, alors, suivant la charge de trafic de réplication, les paquets pouvaient être plus ou moins ralentis, ces ralentissements pouvant engendrer des pertes par "timeout". La seconde raison était que le problème de perte de paquets ICMP n'était pas forcément la seule réponse à notre problème. Depuis le début de l'analyse, certains compteurs montraient des incrémentations anormales. Ces compteurs étaient principalement les compteurs de retransmission et de "out of order".

Nous espérions avoir trouvé la source du problème de performance, mais, la réponse du fournisseur de service ne fut pas une surprise. Effectivement, il appliquait des règles de QoS; les pertes des paquets ICMP étaient donc tout à fait logiques et montraient au contraire que le réseau se comportait comme prévu.

6.5. Elimination du principal défaut

Assez rapidement dans la gestion de l'appel, je me suis aperçu de l'incrémentation des compteurs TCP Out-Of-Order et Retransmission. Suite aux investigations menées jusque là,

[23] ICMP : Internet Control Message Protocol. Protocole de la 3ème couche OSI (comme le protocole IP) utilisé pour les messages de contrôle et d'erreurs.

je savais désormais que la recherche du défaut s'orientait maintenant vers un problème réseau (et non FC) et que l'incrémentation des compteurs n'était probablement pas une conséquence des coupures de tunnels TCP ou autres. Ainsi, l'environnement du problème se réduisait à l'infrastructure et à la configuration entre les interfaces Gigabit Ethernet des commutateurs MDS. Même si le compteur de retransmission pouvait avoir une relation avec les pertes de paquets ICMP, l'incrémentation du compteur Out-Of-Order, quant à lui, montrait l'utilisation de plusieurs chemins avec des temps de transmissions différents, puisque les paquets TCP arrivaient dans le désordre. Il me fallait maintenant vérifier les compteurs TCP des interfaces GigE impliquées dans cette partie en utilisant la commande "***show ips stats tcp all***".

► Création du delta entre deux collections des commandes *show ips stats tcp all*:

-collection 1: `Thu Mar 20 10:49:15 UTC 2008`

```
TCP Statistics for port GigabitEthernet9/2
    TCP send stats
      37543 segments, 1969164 bytes
      20637 data, 16864 ack only packets
      1 control (SYN/FIN/RST), 0 probes, 0 window updates
      42 segments retransmitted, 5300 bytes
      42 retransmitted while on ethernet send queue, 0 packets split
      0 delayed acks sent
    TCP receive stats
      40184 segments, 14945 data packets in sequence, 1590888 bytes in sequence
      17949 predicted ack, 14858 predicted data
      0 bad checksum, 0 multi/broadcast, 0 bad offset
      0 no memory drops, 0 short segments
      424 duplicate bytes, 1377 duplicate packets
      0 partial duplicate bytes, 0 partial duplicate packets
      47332 out-of-order bytes, 545 out-of-order packets
      0 packet after window, 0 bytes after window
      0 packets after close
      19022 acks, 1969164 ack bytes, 0 ack toomuch, 6880 duplicate acks
      1 ack packets left of snd_una, 0 non-4 byte aligned packets
      31 window updates, 0 window probe
      1 pcb hash miss, 1 no port, 0 bad SYN, 51 paws drops
…/…
```

Figure 20: Analyse des compteurs TCP - Collection 1.

-collection 2: `Fri Mar 21 14:51:21 UTC 2008`

```
TCP Statistics for port GigabitEthernet9/2
    TCP send stats
      3158729 segments, 20205240 bytes
      112239 data, 2989799 ack only packets
      0 control (SYN/FIN/RST), 0 probes, 0 window updates
      56691 segments retransmitted, 20967012 bytes
      55066 retransmitted while on ethernet send queue, 428 packets split
      24000 delayed acks sent
    TCP receive stats
      3419125 segments, 108392 data packets in sequence, 84036260 bytes in sequence
      41081 predicted ack, 108139 predicted data
      0 bad checksum, 0 multi/broadcast, 0 bad offset
      0 no memory drops, 0 short segments
      915154332 duplicate bytes, 859584 duplicate packets
      0 partial duplicate bytes, 0 partial duplicate packets
      2195634328 out-of-order bytes, 2081069 out-of-order packets
      0 packet after window, 0 bytes after window
      0 packets after close
      78380 acks, 19845976 ack bytes, 0 ack toomuch, 1061408 duplicate acks
      8736 ack packets left of snd_una, 0 non-4 byte aligned packets
      16923 window updates, 0 window probe
      0 pcb hash miss, 0 no port, 0 bad SYN, 9714 paws drops
…/…
```

Figure 21: Analyse des compteurs TCP - Collection 2.

Il est donc possible de se rendre compte qu'en l'espace de 28h, un nombre important de retransmissions et de paquets délivrés dans le désordre sont apparues sur la communication entre les commutateurs Com-A2 et Com-B2. Si on compare le nombre de segments transmis avec le nombre de retransmissions, on s'aperçoit que, sur cette période, il y a eu environ 2% de retransmissions. Avec un taux de 2% de retransmissions, les performances réelles au niveau FCIP sont dramatiquement réduites et il faut alors compter une perte de performance de plus de 50%. Dans ces conditions, et puisque la liaison était stable, le problème de performance était bien dû à des retransmissions de segments entre les interfaces GigE des commutateurs.

Suivant les types d'infrastructures, les paquets TCP peuvent arriver dans le désordre, mais par spécifications, le protocole TCP est capable de remettre les trames dans l'ordre. Cette action est possible car chaque paquet a un marqueur qui l'identifie dans la transmission. Dans l'hypothèse où des paquets seraient transmis dans le désordre, certains compteurs seraient alors incrémentés.

---

*The **TCP** must recover from data that is damaged, lost, duplicated, or **delivered out of order** by the internet communication system. This is achieved by assigning a **sequence number** to each octet transmitted, and requiring a positive acknowledgment (ACK[24]) from the receiving TCP. If the ACK is not received within a timeout interval, the data is retransmitted. At the receiver, the sequence numbers are used to correctly order segments that may be received **out of order** and to eliminate duplicates.*

Informations issues de la RFC793.

Ceci est possible en utilisant, là encore, des mémoires tampons permettant de stocker momentanément les paquets à retransmettre et de signifier dans le message ACK quels paquets ont été reçus dans l'ordre. Dans l'hypothèse de segments reçus dans le désordre, les compteurs "***out-of-order bytes***" et "***out-of-order packets***" vont s'incrémenter. Ensuite si ces paquets sont délivrés dans le désordre, il est possible que des retransmissions soient nécessaires. Dans ce cas, le compteur "***segments retransmitted***", va lui aussi s'incrémenter renseignant ainsi les statistiques de transmissions.

Toutefois, le compteur "***Duplicate acks***" attirait mon attention, il était bien plus important que le "ACK" standard. Pour environ 3 millions de segments envoyés, l'interface avait reçu plus d'1 million de "*Duplicate ACK*" contre seulement 78 miles ACKs. Le compteur *Duplicate ACK* s'incrémente lorsque le récepteur demande une retransmission de paquets. Les Duplicate ACKs sont aussi utilisés par la fonctionnalité TCP "Fast Retransmit", qui a pour but d'éviter l'attente de timeout avant de retransmettre. Ainsi, si un paquet est reçu dans le désordre, le récepteur émet un Duplicate ACK pour ce numéro de segment. Si trois Duplicate ACK consécutifs sont reçus alors, le transmetteur retransmet le segment manquant sans attendre le timeout.

[24] ACK : Acknowledgement : est un message envoyé par le récepteur afin de notifier le transmetteur que les paquets « n » ont bien été reçus.

***A TCP receiver should send an immediate duplicate ACK when an out-of-order segment arrives**. The purpose of this ACK is to inform the sender that a segment was received out-of-order and which sequence number is expected.*

***After receiving 3 duplicate ACKs**, TCP performs a retransmission of what appears to be the missing segment, without waiting for the retransmission timer to expire.*

Informations issue de la RFC2581.

J'ai compris que beaucoup de trames étaient reçues dans le désordre. De plus, très souvent, la durée, avant d'avoir reçu la trame manquante était suffisamment longue pour activer le "fast retransmit" et ainsi demander la retransmission d'une trame, qu'elle soit effectivement perdue ou simplement trop retardée.

A ce stade de l'appel, j'avais suffisamment d'arguments pour impliquer l'équipe réseau dans la gestion de la partie WAN. En effet, de par ma spécialité et mon cursus, j'avais été capable d'isoler le problème. Mais dans le cadre de cette escalade, il fallait impérativement avoir la confirmation officielle des experts support réseau HP. De la même manière, et puisque l'appel était escaladé au haut management chez HP et chez le client, j'avais élevé l'appel à l'équipe d'Ingénierie HP basée aux Etats-Unis. Ceci permettait qu'ils confirment mon analyse et aussi qu'ils travaillent en collaboration avec le support Cisco, afin de mettre en place l'équipe technique complète pour assurer l'explication et confirmer mes analyses fournies jusque lors. De plus, si je n'étais pas capable de déterminer l'origine du défaut, ou si mon analyse n'était pas la bonne, il fallait que je puisse avoir recours aux équipes dédiées afin d'assurer les réponses techniques liées à l'escalade. De plus, d'un point de vue management, cela montrait aussi que la partie technique était adressée au plus haut point et que le constructeur était impliqué dans la gestion de l'appel. Cela représente également une des tâches importantes de mon travail. Il est primordial d'être capable d'impliquer les équipes supports supérieures en temps voulu, en fournissant une analyse technique pointue et de qualité, afin de leur adresser clairement les besoins.

Une fois le problème explicité et après avoir fait l'inventaire des actions menées et en cours, ainsi que l'analyse des logs, plusieurs points de vues ont émergé. Nous étions tous d'accord sur le constat, mais l'identification des causes possibles étaient différentes.

-**Le support SAN Cisco et l'Ingénierie SAN HP** présumaient que les Out of Order étaient une conséquence des retransmissions, dont la source était un problème réseau (matériel ou configuration) et qu'il fallait que le client travaille avec le fournisseur réseau afin de résoudre ce problème.

-**Le support réseau HP et moi-même** pensions que le problème de retransmission était plutôt une conséquence du design et de la cohabitation des protocoles FC et IP (pouvant potentiellement venir d'un problème sur le réseau). Selon nous, il fallait agir sur la configuration des commutateurs afin de pallier ce problème.

-**Le client et le fournisseur de services** maintenaient que le réseau était sans problème et que le souci venait soit des commutateurs, soit des baies de stockage. Pour lui, le support HP essayait de déplacer le problème vers la partie réseau afin de se dégager de l'appel.

Du même coup, le client devenait de plus en plus sensible quand on évoquait la partie réseau.

Tout en considérant ces trois points de vue, il fallait pouvoir avancer et permettre l'application d'un plan d'actions le plus cohérent et le plus acceptable aux yeux de tous. Etant l'interface privilégiée entre l'équipe technique et l'équipe de management, m'incombait la tâche importante de définir les étapes suivantes du dépannage.

J'ai donc décidé de mettre en place une conférence téléphonique avec les interlocuteurs principaux. Ainsi, j'ai tout d'abord contacté le responsable du réseau chez le client et je lui ai expliqué mon point de vue et mon approche, le rassurant sur le fait que la conférence n'avait pas pour but de l'influencer afin de déplacer le problème vers le réseau, mais plutôt de permettre à chacun d'exposer ses hypothèses et de permettre une résolution rapide de ce dilemme. De plus, j'ai mis en place des outils internes de partage d'écran et prise de connexion à distance afin de permettre des récupérations de logs et des configurations en direct. J'ai ainsi contacté tous les intervenants experts techniques afin de travailler en équipe restreinte afin de faciliter la communication. J'ai aussi pris la précaution de demander au responsable du compte client d'être présent dans le but d'assurer la partie gestion de l'escalade. Après plusieurs heures de conférences, nous arrivions tous à la conclusion qu'effectivement le réseau se comportait correctement et qu'il fallait agir sur la configuration FCIP des commutateurs afin de corriger la réception des segments dans le désordre.

Si le problème était effectivement la réception de données dans le désordre, il fallait en priorité éviter l'utilisation de plusieurs chemins entre les interfaces d'émissions et de réceptions. La figure ci-dessous illustre les chemins empruntés par les paquets provenant de chaque interface GigE.

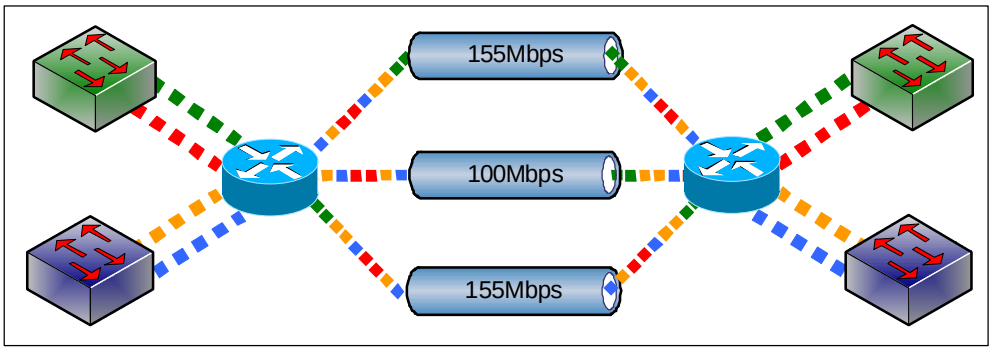


Figure 22: Représentation des chemins empruntés initialement.

Ainsi, et contrairement à la configuration actuelle, nous allions forcer l'utilisation d'un profil FCIP sur une interface GigE puis, forcer la transmission sur un seul tunnel STM1 par fabric. Nous avons donc reconfiguré les profils FCIP afin d'avoir une bande passante de 155 Mbps au maximum ; ensuite le client a reconfiguré ses routeurs afin de forcer le trafic à n'utiliser qu'un seul tunnel par fabric. La figure suivante illustre les chemins empruntés par les paquets provenant de chaque interface GigE une fois la modification apportée.

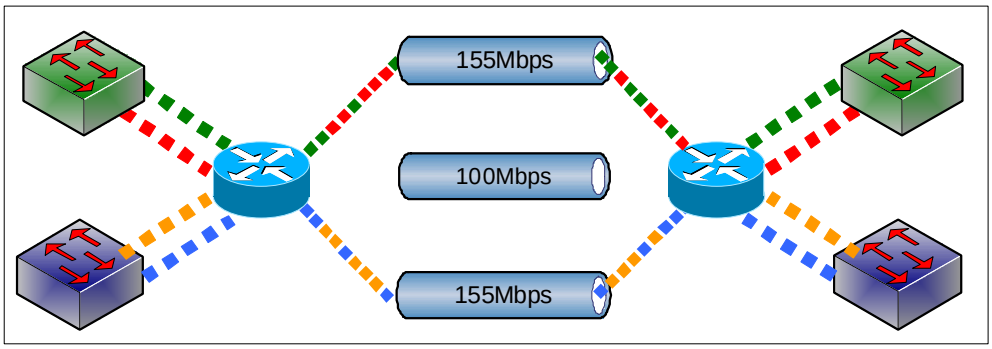


Figure 23: Représentation des chemins empruntés suite à la première reconfiguration.

Suite à l'application de cette nouvelle configuration, l**e résultat fut immédiat, les compteurs out of order et retransmission cessèrent de s'incrémenter instantanément.** Nous venions de franchir une étape importante dans la résolution de l'appel, car, enfin, la liaison était non seulement stable, mais les performances avaient enfin progressé fortement.

Toutefois, même si nous avions pu nettement améliorer la situation, le problème n'était pas complètement résolu. En fait, le design que nous avions appliqué avait comme principal défaut l'utilisation de seulement deux tunnels STM1 (un par fabric), autorisant ainsi une bande passante globale de 310 Mbps, alors qu'il restait le troisième tunnel partiellement disponible pour la réplication et qui offrait 100 Mbps supplémentaire. Si on additionnait à cette limitation le fait que la compression et l'accélération n'étaient pas activées, les performances n'étaient pas suffisantes pour permettre la réplication des données les plus volumineuses. Il fallait, tout en gardant cette solution, permettre l'utilisation des 100 Mbps disponibles et optimiser la configuration afin de garantir les performances pleines et entières, ce qui était le critère de résolution de l'appel.

7. Optimisations

La partie la plus importante de l'escalade venait d'aboutir. Nous venions, après un travail intensif de 3 jours, de confirmer et de corriger le problème principal. L'appel n'en était pas pour autant terminé, puisque les réplications n'étaient pas complètement possibles. Ainsi, même si la situation s'était nettement améliorée, il fallait encore fournir un travail important de façon à obtenir les performances optimales.

7.1. Première optimisation

L'objectif de la première optimisation était de permettre l'utilisation des 100 Mbps supplémentaires, sans recréer les conditions conduisant à la génération de trames reçues dans le désordre. J'ai donc travaillé sur différentes possibilités de design puis j'ai présenté mes propositions au support Cisco avant de valider la meilleure option et de la mettre en place sur l'infrastructure du client.

7.1.1. Analyse de la source du problème

Le cahier des charges était le suivant:

> **Intégrer le troisième tunnel STM1 de 100 Mbps de façon à ce qu'il soit partagé équitablement sur les deux fabrics, pour éviter un déséquilibre de charge sans pour autant générer des out of order sur le réseau.**

Cette mission semblait assez simple au premier abord ; en effet, il suffisait de déplacer la seconde interface GigE de chaque commutateur et de faire en sorte que le trafic généré par ces interfaces passe au travers de ce troisième tunnel. Il fallait donc que le trafic généré par ces interfaces ne dépasse pas 50 Mbps, de façon à s'assurer que les 100 Mbps disponibles soient partagés entre les deux fabrics. En même temps, il fallait donc forcer ce trafic à ne prendre que ce tunnel STM1, sinon, la condition de création d'out of order serait réapparue. Ce qui signifiait que les tunnels STM1 dédiés à la réplication (tunnels de 155 Mbps) n'allaient transporter que le trafic venant d'une seule interface GigE de chaque commutateur. La figure suivante décrit le concept utilisé afin de répondre à ce besoin.

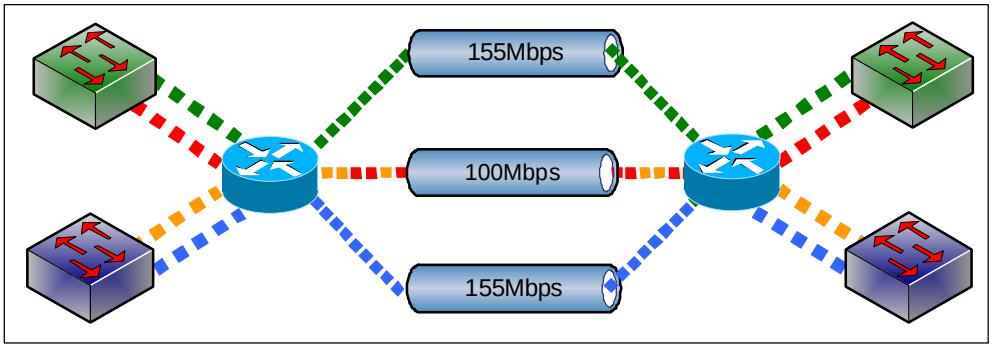


Figure 24: Représentation des chemins empruntés avant la première optimisation.

Dans la configuration actuelle, cela signifiait que sur les deux interfaces GigE de chaque commutateur, une interface transporterait du trafic jusqu'à un débit maximum de 155 Mbps et sur l'autre interface un maximum de 50Mbps. Toutefois, avant d'appliquer cette configuration

sur l'infrastructure, j'avais pris la précaution de discuter avec l'équipe d'engineering HP et le support Cisco, car je m'interrogeais sur la possibilité d'avoir des interfaces FCIP configurées avec des valeurs de bande passante maximum différentes dans un même "port-channel". En effet, dans la documentation Cisco, tous les exemples montrent des configurations symétriques avec des interfaces utilisant la même valeur de bande passante maximum. Je me demandais donc s'il était possible de faire cohabiter plusieurs interfaces FCIP utilisant des interfaces GigE différentes avec des valeurs de bandes passantes différentes et m'interrogeais sur les conséquences de cette cohabitation.

Cette question était loin d'être anodine, puisque d'un point de vue connexion TCP, il ne devait pas y avoir de raisons pour que ce type de configuration ne soit pas possible. En effet, dans cette hypothèse, puisque les tunnels TCP sont initialisés entre les interfaces FCIP, chaque tunnel est séparé et peut se configurer indépendamment des autres tunnels. Mais en même temps, lors de la configuration d'un port-channel, il faut que la configuration des interfaces soit identique, sinon le port-channel ne s'active pas. Puisque je ne trouvais aucune trace de configuration similaire dans les documents constructeurs, j'ai donc préféré poser la question au support Cisco.

Effectivement, cette interrogation n'était pas simple, car ni l'Engineering HP, ni le support Cisco ne pouvait répondre formellement à cette question. Cisco a donc travaillé en interne avec les développeurs afin de déterminer s'il était possible de configurer plusieurs interfaces FCIP avec des valeurs de bandes passantes différentes sur le même module au sein d'un port-channel. Au final, pour des raisons de design interne à la carte permettant l'utilisation des fonctions FCIP, les valeurs maximum de bande passante, même si elles sont différentes, sont alors limitées en interne de façon à ne pas dépasser la plus faible des valeurs maximales. Ainsi, la première proposition que j'avais élaborée n'était pas applicable, car il y aurait eu un maximum de bande passante de deux fois 50Mbps par commutateur, ce qui était bien plus bas que la solution appliquée en ce moment.

Dans le cahier des charges, il était possible d'ajouter une nouvelle contrainte fondée sur la similitude des valeurs maximum des bandes passantes des interfaces FCIP. Puisque nous étions limités à 50 Mbps pour le tunnel partagé, cela impliquait que les interfaces FCIP devraient être configurées toutes avec la même valeur de 50 Mbps pour la bande passante maximum. Ou alors, une solution alternative était de ne pas utiliser la fonction port-channel, ce qui avait comme inconvénient de diminuer fortement la tolérance de la fabric face à une perte de tunnel TCP. Nous avons donc décidé de modifier la configuration des interfaces FCIP afin d'optimiser les performances. Il fallait ainsi diviser les liens à 155Mbps avec des tunnels TCP permettant une bande passante maximale d'environ 50Mbps. Ainsi, chaque lien à 155 Mbps devait supporter trois tunnels TCP de 50 Mbps maximum et le lien à 100 Mbps devait en supporter deux. Ce qui amenait au total à quatre tunnels TCP par fabric, soit quatre profiles FCIP par commutateur.

7.1.2. Configuration associée

Pour répondre à cette configuration, deux options étaient possibles. La première était d'associer une interface FCIP par interface GigE. Dans ce cas, puisqu'il fallait quatre interfaces FCIP, cela nécessitait quatre interfaces GigE. Seulement, cela impliquait encore d'autres modifications côté réseaux, y compris l'achat de matériels. La seconde option était de configurer quatre interfaces FCIP et de continuer d'utiliser les deux interfaces GigE. En fait, sur le type de modules utilisés par le client, il était possible de faire cette configuration, car les interfaces GigE peuvent supporter jusqu'à trois interfaces FCIP chacune. La figure ci-contre représente le cheminement des paquets entre le commutateur FC et l'élément réseau suivant.

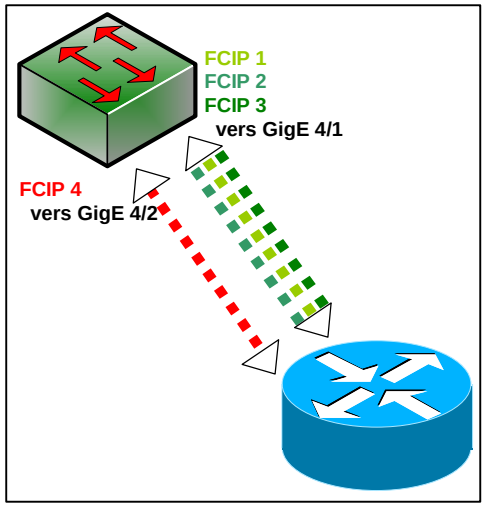


Figure 25: Représentation des chemins empruntés à l'issue de la première optimisation.

Pour la valeur de la bande passante maximum, il se posait aussi la question d'en-têtes supplémentaires au niveau SDH, ou bien de l'occupation de tunnel TCP de contrôle,… Pour éviter d'autres problèmes de saturation, j'ai proposé la réduction de la valeur maximale à un niveau de 47 Mbps, puis la configuration de la valeur minimale à 40 Mbps. Nous savions que 47 Mbps était une valeur assez basse, mais qui présentait l'avantage de ne pas avoir de saturations et qui permettait une bande passante totale de 8 x 47 = 376 Mbps.

Un autre paramètre avait été discuté, il s'agissait du RTT. Il avait été vu, dans les phases de tests et dans les différentes discussions avec le client, que le RTT pouvait varier entre 70 et 120 ms mais qu'il était fréquemment aux alentours de 84 ms. Toutefois, pendant les investigations, il était monté jusqu'à la valeur de 100 ms. Nous proposions donc aussi de revoir ce paramètre et de passer à 100 ms au lieu de 84 ms. Cela permettait de mieux configurer la fenêtre de transmission et ainsi d'éviter des saturations.

J'ai dû par la suite appliquer cette nouvelle configuration à tous les commutateurs de la fabric. La configuration de Com-B2 était alors la suivante:

```
fcip profile 5
  port 3225
  ip address 10.249.0.22
  tcp max-bandwidth-mbps 47 min-available-bandwidth-mbps 40  round-trip-time-ms 100

fcip profile 6
  port 3226
  ip address 10.249.0.23
  tcp max-bandwidth-mbps 47 min-available-bandwidth-mbps 40  round-trip-time-ms 100

fcip profile 7
  port 3227
  ip address 10.249.0.23
  tcp max-bandwidth-mbps 47 min-available-bandwidth-mbps 40  round-trip-time-ms 100

fcip profile 8
  port 3228
  ip address 10.249.0.23
  tcp max-bandwidth-mbps 47 min-available-bandwidth-mbps 40  round-trip-time-ms 100

interface port-channel 1
  channel mode active

interface fcip5
  channel-group 1 force
  use-profile 5
  peer-info ipaddr 10.251.0.22 port 3225

interface fcip6
  channel-group 1 force
  use-profile 6
  peer-info ipaddr 10.251.0.23 port 3226

interface fcip7
  channel-group 1 force
  use-profile 7
  peer-info ipaddr 10.251.0.23 port 3227

interface fcip8
  channel-group 1 force
  use-profile 8
  peer-info ipaddr 10.251.0.23 port 3228
```

Figure 26: Exemple de configuration d'un commutateur pour appliquer la première optimisation.

Une fois cette nouvelle configuration appliquée, la situation était redevenue stable et les performances, bien que n'étant toujours pas à la valeur maximale, permettaient à nouveau la réplication intégrale des données d'un site vers l'autre quelle que soit la volumétrie. Toutefois, étant donné les performances faibles, il fallait un temps important pour pouvoir finaliser toutes les réplications. Quoi qu'il en soit, à ce stade de l'appel, la criticité et l'escalade ont pu être diminuées, l'appel redevenant un appel normal, ne nécessitant plus la poursuite du travail en astreinte.

Il restait néanmoins plusieurs axes d'améliorations. Le premier était l'upgrade des commutateurs afin de permettre la réactivation des fonctionnalités de compression et d'accélération, ce qui devait nous amener à la finalisation de l'escalade et donc à la clôture de l'appel.

7.2. Upgrade des commutateurs

L'upgrade d'un commutateur, bien qu'il soit transparent sur ces modèles, est une tâche délicate. En effet, le trafic peut continuer à être traité sans pertes de performances pendant la mise à jour logicielle. Même si les cartes processeurs sont redondantes, suivant les versions à upgrader ou suivant les problèmes potentiellement rencontrés lors de l'opération, il peut y

avoir des interruptions de trafic. Puisque nous venions tout juste de stabiliser l'environnement, il fallait fournir le plus grand soin à cette opération afin qu'elle puisse se dérouler dans les meilleures conditions.

7.2.1. Analyse et besoins

J'ai donc fourni une procédure détaillée sur l'opération à effectuer. Cisco possède des documents très complets sur le mode opératoire à mettre en place pour une mise à jour, mais ce n'était pas ce type de documents que l'équipe locale recherchait. En fait, il m'était demandé de couvrir tous les points possibles, potentiellement risqués pour l'infrastructure lors de la mise à jour. Ce type de documents n'existe pas et le seul moyen de le créer est de lister tous les problèmes possibles ou du moins connus puis, de préciser ce qu'il faut faire pour les éviter.

Ce document était extrêmement important car maintenant que les réplications fonctionnaient, il ne fallait plus perturber le trafic. Il y avait donc une très forte visibilité sur cette action au niveau du haut management client et HP, ce qui augmentait d'autant plus la complexité du travail à fournir. De plus, je devais alors créer un document qui tient plus du consulting que du support réactif. Il m'était presque impossible de travailler avec le support Cisco ou l'engineering HP, trop occupés sur d'autres appels critiques. J'ai donc élaboré le document que j'ai ensuite présenté en interne à mon équipe puis discuté avec le support Cisco, qui n'a eu que peu d'observations à ajouter.

7.2.2. Procédure et mode opératoire

La procédure comportait les différentes étapes à exécuter avant l'opération afin de s'assurer que les commutateurs seraient prêts pour accepter la mise à jour sans être perturbés. Elle présentait aussi les liens permettant l'accès aux informations plus détaillées aux scripts, aux applications, aux notes nécessaires pour accomplir les différentes actions.

Je préconisais aussi de faire l'action commutateur par commutateur et fabric par fabric. Ainsi, si nous avions dû arrêter l'opération soit par manque de temps, soit parce qu'un commutateur posait problèmes, il était facile de savoir quel était l'état final de la mise à jour. Cette méthode peut paraître évidente mais il est à noter que les commutateurs se trouvaient sur deux sites dans deux pays différents et que je devais bien insister sur l'ordre des opérations afin de s'assurer que les deux équipes ne travaillaient pas simultanément. Comme la mise à jour logicielle avait lieu la nuit, il avait été aussi convenu que j'étais d'astreinte dédiée lors de cette opération. Ceci permettait de fournir un support immédiat en cas de problème.

J'avais aussi insisté pour que sur site il y ait des cartes de remplacements en cas de problème lors de l'upgrade de certains modules.

Au final, cette opération s'est déroulée sans problèmes majeurs et dans les temps impartis. Ainsi, il a été possible dès le lendemain de réactiver les fonctionnalités de compression et d'accélération afin d'obtenir les performances maximales.

La procédure fournie se trouve en Annexe 2, page 83.

7.3. Seconde optimisation – finalisation

La seconde phase d'optimisation avait pour but de mettre en œuvre les fonctionnalités qui permettaient de retrouver les performances d'origine et ainsi de pouvoir clôturer l'appel. Les fonctions à réactiver étaient la compression et l'accélération en écriture.

7.3.1. Analyse de la source du problème

Ces deux options sont très souvent utilisées pour améliorer les performances. En effet, la compression permet de compresser la partie FC de la trame, y compris les en-têtes TCP et FCIP. Puis, le protocole ajoute un en-tête (IPComp[25]) de 4 octets définissant les informations liées à l'algorithme de compression. La figure ci-dessous montre la structure d'une trame FCIP non compressée et celle d'une trame compressée.

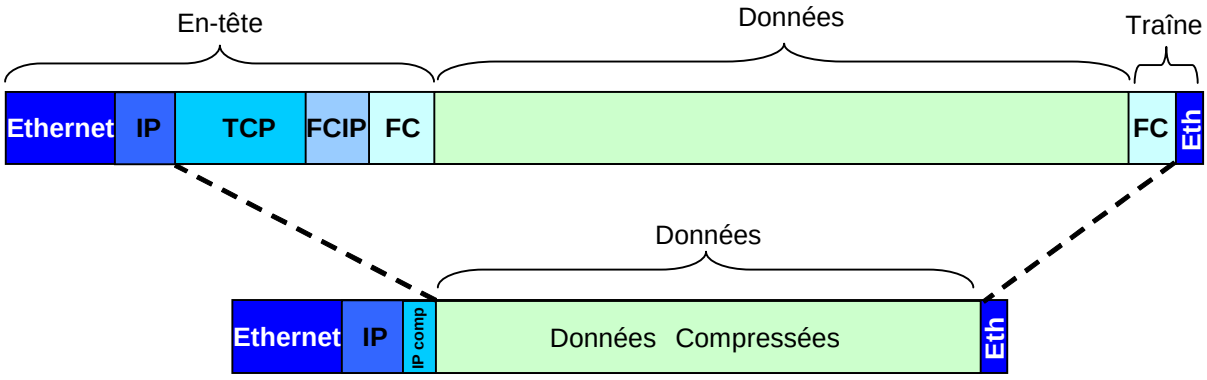


Figure 27: Représentation de la trame sans et avec la compression.

Pour la compression, plusieurs modes sont possibles, suivant si on veut compresser beaucoup de données pour un réseau à faible bande passante ou si on veut faiblement compresser les données pour un réseau à forte bande passante. Le principe est de trouver le meilleur compromis afin d'optimiser le débit. Car plus la compression est importante, plus les processeurs de la carte sont utilisés pour accomplir cette compression. La saturation des processeurs peut induire un ralentissement dans le traitement des trames et donc ralentir le trafic. Suivant les caractéristiques du réseau, le mode de compression utilisé et le contenu de la trame d'origine, il est possible d'atteindre une trame compressée d'un rapport 10. Dans les versions logicielles récentes, il y a trois modes de compression:

Mode 1: Faible compression pour des réseaux haut débit, supérieurs à 25 Mbps
Mode 2: Compression modérée pour des débits de 10 Mbps à 25 Mbps.
Mode 3: Forte compression pour des débits inférieurs à 10 Mbps

Dans l'environnement du client, la compression de mode 1 était celle à sélectionner étant donné que la bande passante par tunnel TCP était supérieure à 25 Mbps.

[25] IPComp : IP payload compression protocol – aussi appelé IPPCP. C'est l'en-tête contenant les informations liées aux données compressées.

La seconde option à activer était l'accélération en écriture (WA[26]). Cette fonctionnalité simplifie les échanges de données au niveau du protocole SCSI[27]. Lors de l'établissement de la connexion ou lors de l'échange de certaines commandes, l'émetteur attend la réponse du récepteur avant d'émettre les trames suivantes. Suivant le temps de latence du réseau, principalement lors de l'utilisation de liaison FCIP pouvant utiliser l'infrastructure d'un réseau WAN sur de longue distance, il est possible que le temps d'attente pour l'acquittement soit trop long. Dans ce cas, les performances peuvent être affectées puisque le taux de transfert n'est pas optimisé. Ainsi, la fonction d'accélération en écriture permet de ne pas attendre la réponse du récepteur. Cette réponse, pour se conformer aux normes régissant le protocole, doit pourtant arriver au transmetteur avant de valider l'émission des autres trames. Cet acquittement se fait depuis le commutateur MDS ayant la fonctionnalité WA activée. L'amélioration des performances attendue est environ deux fois supérieure au taux de transfert sans la fonctionnalité activée.

7.3.2. Configuration associée

Une fois ces deux fonctionnalités activées, il était possible d'espérer atteindre des performances proches de la bande passante totale, soit environ 376 Mbps[28]. Toutefois, même avec le maximum de données à transférer, il n'était pas possible d'atteindre plus de 250 Mbps. Plusieurs tests ont été faits afin de trouver le problème. La difficulté principale résidait dans le fait qu'il était difficile de déterminer quel élément limitait la bande passante : l'application, les processeurs des baies de stockage, le réseau, la configuration des commutateurs MDS,…

Il fallait donc que chaque équipe travaille de son côté pour déterminer l'élément perturbateur dans la chaîne de transmission. Ainsi, j'ai recontacté le support Cisco pour analyser en détail les logs des commutateurs. Après plusieurs échanges de données et aussi des discussions sur le design j'ai pointé un document qui me paraissait intéressant dans la compréhension des fonctionnalités liées aux modules. Il s'agissait d'un tableau reprenant les débits possibles suivant les modules employés et le mode de compression utilisé.

Module	**Mode de compression**			
	Mode 3	**Mode 2**	**Mode 1**	
IPS-4 IPS-8	Débit de l'application Max: 69 Mbps	Débit de l'application Max: 182 Mbps	Débit de l'application Max: 334 Mbps	
Bande passante	0-10 Mbps	10-25 Mbps	25-100 Mbps	<1 Gbps

Figure 28: Tableau montrant les débit suivant les modes de compressions et les modules utilisés.

Le tableau ci-dessus pouvait donc s'interpréter de la manière suivante:
Avec l'utilisation d'un module IPS-8, si le mode de compression 1 est utilisé, il ne sera pas possible d'avoir un débit supérieur à 334Mbps même si la bande passante est supérieure à 100 Mbps.

[26] WA : Write Accélération (Accélération en écriture)
[27] Small Computer System Interface : Protocole de couche haute définissant l'échange de données entre un émetteur et un récepteur.
[28] Il y avait 4 interfaces FCIP par fabric, donc 8 interfaces au total ayant une bande-passante Max de 47Mbps, soit 8x47Mbps=376Mbps

Cette limitation était appliquée par la carte. Je me suis donc interrogé sur les raisons de cette limite et j'ai posé les questions suivantes au support Cisco: pourquoi avions-nous de telles contraintes et était-il possible que ces limitations puissent être en relation avec le problème de performance? La réponse était simple et correspondait à l'explication des trois modes de compression. La limite est liée à l'utilisation des processeurs dans les cartes offrant la fonctionnalité FCIP. Dans les cartes IPS-4 ou 8, la compression se fait de façon dite "logicielle[29]" au niveau des processeurs de la carte; il y a deux ports GigE par processeur, ce qui, suivant les configurations peut amener à des limitations dans le débit par port. Si les ports utilisés dans la connexion FCIP partageaient le même processeur, les performances seraient directement limitées. Dans notre situation, nous utilisions à chaque fois, les deux ports consécutifs sur les modules qui, par design, partageaient les mêmes processeurs. Ainsi, après avoir déplacé la seconde connexion sur un autre port GigE il était possible d'avoir de meilleurs résultats. Il y avait un gain de performance d'environ 20- 40%. Il était possible d'atteindre environ 300-350 Mbps, ce qui nous amenait enfin à l'utilisation presque maximale de la bande passante. Néanmoins les cartes utilisées ne permettaient pas beaucoup plus de performances à cause de la limite induite par l'utilisation de la compression logicielle. Pour améliorer les performances il faudrait utiliser des cartes de nouvelle génération utilisant la compression matérielle.

Cependant, il subsistait deux points qui faisaient plafonner les performances. Le premier était lié aux tests de performances fait par les lab Cisco. Ils ont testé avec leurs modules que, sur une liaison à 155 Mbps sans aucune retransmission, l'utilisation réelle de la bande passante était d'environ 144 Mbps. Ceci pouvait être dû aux autres encapsulations (SDH,…) mais aussi aux signaux de contrôle, limitation du module… Dans un réseau même parfait, il existe toujours quelques retransmissions et il était illusoire de croire qu'il serait possible d'atteindre les valeurs maximales. Enfin un autre point pouvait assez facilement améliorer les performances. Il était lié à la fragmentation des trames.

[29] Il existe deux options pour utiliser des applications à ce niveau, soit de façon « logicielle » en utilisant une couche logicielle souvent associée à des processeurs, … soit de façon « matérielle » en utilisant des composants appelé ASIC incorporant les opérations à effectuer. Dans ce cas, les actions utilisant le « matériel » sont généralement plus rapides.

7.4. Schéma logique de l'infrastructure après la résolution.

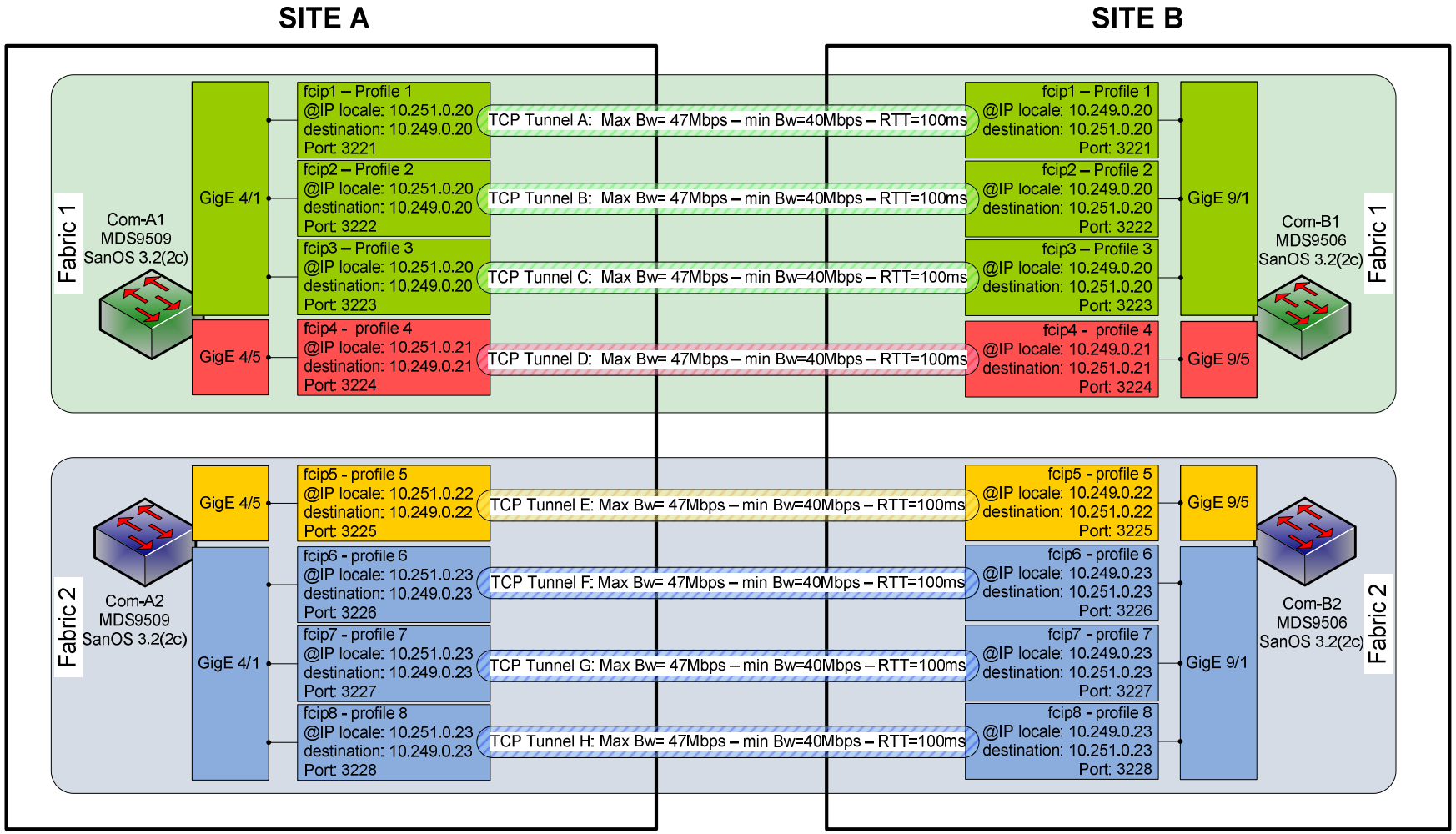


Figure 29: Schéma de l'infrastructure (couche logique) après la résolution de l'appel.

7.5. Prochaines étapes – amélioration

Dans les dernières améliorations qu'il était possible d'apporter, je proposais deux approches. La première était l'utilisation de trames plus grande sur le réseau pour atteindre de meilleures performances. La seconde était d'utiliser certaines fonctionnalités afin de permettre un meilleur comportement des commutateurs dans la fabric. Ces propositions d'améliorations ont été demandées en fin d'escalade en vue d'être mises en œuvre ultérieurement.

7.5.1. Taille des trames

Comme expliqué en page 11 au paragraphe 3.2.5, les trames FC sont encapsulées successivement avant de pouvoir être envoyées sur le réseau. Ces encapsulations impliquent des tailles de trames de plus en plus grandes, mais surtout, le format des trames FC n'est pas de façon native compatible avec les trames Ethernet. En effet, la trame FC peut être composée jusqu'à 2148 Octets, alors que, de façon standard, la taille maximale d'une trame Ethernet sur les réseaux est de 1500 Octets. Il s'agit du MTU[30]. Ci-dessous le schéma représentant une trame FCIP avec les en-têtes des protocoles successifs.

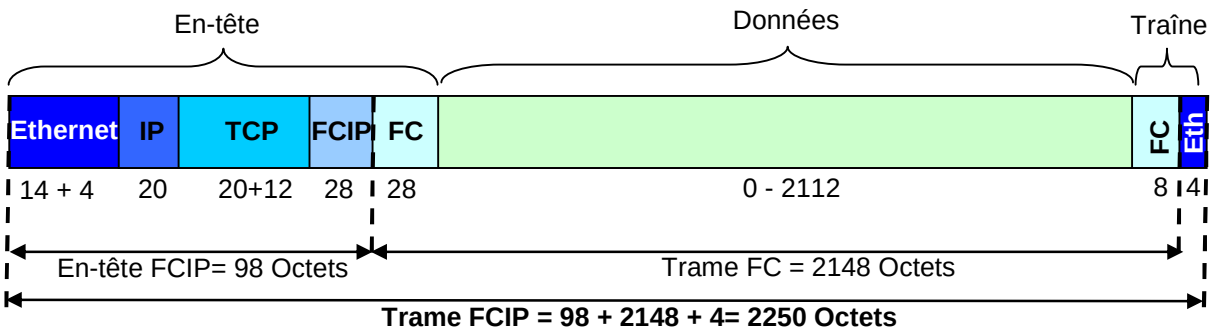


Figure 30: Composition d'une trame FCIP.

La partie « traîne » comprend généralement des marqueurs de fin de trame et des informations relatives à la vérification de l'intégrité de la trame (CRC[31]). Ainsi, si la trame est supérieure au MTU du réseau, il faudra fragmenter la trame en deux, de façon à la transmettre entière de bout en bout du réseau. Ceci réduit les performances. Il existe donc la possibilité sur les réseaux récents de configurer le MTU avec une taille supérieure, on parle alors de "jumbo frame[32]". Ainsi, si on utilise un MTU de 2300 Octets, une trame FCIP de 2250 Octets pourra être transmise de bout en bout du réseau sans être fragmentée. Il est tout de même important de retenir que toutes les trames FC ne font pas 2148 Octets et qu'il est possible que le gain de performance associé ne soit pas si important, mais puisse n'être que de quelques pour cents. Cependant, il n'est pas possible d'atteindre des valeurs plus importantes même si la compression est utilisée. En effet, la compression IP n'intervient qu'après la fragmentation de la trame. Il en résulte donc dans ce cas deux trames mais avec une taille plus réduite.

[30] MTU : Maximum Transfer Unit : désigne la taille maximale des trames Ethernet sur le réseau.
[31] CRC : Cyclic Redundancy Check, Control de redondance cyclique.
[32] Jumbo frame : Trame « géante » permettant un MTU de 2300 Octets.

7.5.2. Virtual SAN et Inter-VSAN Routing

La deuxième proposition d'amélioration est liée aux fonctionnalités Virtual SAN et Inter-Virtual SAN Routing, appelées communément VSAN et IVR. Le VSAN est la capacité à faire communiquer des équipements uniquement présents dans ce VSAN, un peu comme un SAN de plus petite taille, d'où le nom de SAN virtuel au sein du SAN physique. Ce concept de VSAN découle du concept de VLAN dans le monde des réseaux. L'un des intérêts des VSAN dans l'infrastructure du client est lié à l'isolation de trafic. Ainsi, il pourrait être possible de créer un VSAN dédié au trafic interne au site et d'avoir un autre VSAN uniquement dédié au trafic de réplications intersites. Dans ce cas, les perturbations, ou événements liés à des équipements dans un VSAN ne perturbent pas les équipements de l'autre VSAN. Une seconde option peut, en plus, être activée; il s'agit de l'IVR. L'Inter VSAN Routing permet de faire communiquer plusieurs VSAN différents. Dans ce cas, on peut utiliser ce qui s'appelle un VSAN de transit sur la partie réseau IP afin d'interconnecter les deux sites de réplication. Ainsi on sépare le trafic de réplication et les instabilités du réseau IP sont isolées au sein de ce VSAN de transit, évitant la propagation de ces perturbations aux autres VSAN. Ce type d'optimisation n'améliore pas réellement les performances mais assure une meilleure perméabilité du trafic et des perturbations associées.

8. Retour d'experience

Les escalades sont fréquentes dans l'organisation support chez HP, mais elles atteignent assez rarement cette intensité. Du fait de cette rareté et du nombre d'équipe organisée autour du support, il est proportionnellement moins fréquent de rencontrer de hautes escalades dans une équipe donnée. Plusieurs processus sont mis en place afin d'assurer au client la bonne prise en charge de son problème. La mise en place des ces processus est harmonisée au niveau mondial pour toutes les technologies, ainsi, il est évident qu'il n'est pas possible à mon niveau de les influencer. Néanmoins, dans ce chapitre j'ai pris la gestion de cet appel comme référence en prenant le recul nécessaire afin d'amener des réflexions sur les mécanismes de gestions des appels et du personnel mis en place dans l'organisation support chez HP.

8.1. Mon rôle dans la gestion de l'appel

J'ai occupé une place importante tout au long de la gestion de l'appel. Ce rôle peut se résumer à être le représentant de l'analyse technique. Cette tache n'est pas réductrice et ne se limite pas au simple fait de communiquer autour des actions de diverses personnes. En fait, il faut être à la fois le porteur et l'instigateur de l'analyse technique et, en même temps, être capable de communiquer et expliquer au management local et au client. Il faut aussi être capable de fédérer une équipe d'experts techniques autour des interrogations et des inquiétudes des équipes locales, ce qui amène parfois à devoir également gérer des compromis quant au travail et aux actions à mener. En effet, il peut arriver que l'approche technique puisse être en décalage avec les décisions prises au niveau management ou bien les demandes du client, il faut alors faire la médiation entre les intervenants.

► Rôle d'expert technique

Etre considéré comme un expert technique dans une technologie donnée demande de prendre le temps de comprendre ce que nous devons être capables de fournir. Les équipes locales ou le support de premier niveau qui font appels à nos services nous considèrent comme tels et nous sommes introduits dans les réunions avec les clients en tant qu'experts. Il faut être capable de répondre au besoin formulé et d'accompagner ces équipes lors de la gestion de l'appel afin de permettre une conduite professionnelle de la crise.

Du fait de la spécificité de l'infrastructure, (SAN intégrant la transmission FCIP) et de la nature du problème (dégradation des performances pour les réplications) je fus naturellement point de contact privilégié lors de l'escalade. J'avais en charge la demande de collecte de données spécifiques, le tri de ces données et leurs analyses afin de pouvoir étayer des hypothèses et donc créer et adapter le plan d'actions. En parallèle de ces tâches, je devais aussi accompagner les équipes locales de management afin de faire la communication vers le management supérieur et vers les équipes techniques du client.

Ce rôle doit rester inchangé même lorsqu'on élève un appel à d'autres ressources. En effet, une fois l'Ingénierie ou le support constructeur engagé dans l'appel, il faut rester complètement impliqué et ne pas se désengager des analyses techniques. Puisqu'ils ont accès à des ressources que nous n'avons pas au niveau N2, il est tentant de leur laisser exclusivement ce rôle. Toutefois, cette approche est très risquée car dans ce cas, il n'est plus possible d'avoir ce rôle d'intermédiaire qui consiste à pouvoir filtrer les

informations et les remettre en forme ou bien confronter aussi les analyses afin d'éviter des retours ou des conclusions qui ne correspondent pas à la réalité du terrain. En même temps, on assure aussi que toutes les informations provenant des équipes locales sont pertinentes, cohérentes et complètes, ce qui permettra aux équipes d'Ingénierie et support constructeur de pouvoir travailler.

► Rôle de communiquant

En plus de ce rôle d'expert technique que j'ai tenu jusqu'à la clôture de l'appel, j'ai eu à prendre en charge la communication des analyses vers les équipes locales techniques et le management. Devoir communiquer vers les équipes de managements est inhabituelle dans mon travail. Généralement ce rôle est assuré par le responsable de compte client ou à un ingénieur technique dédié à ce client. Or dans le cas présent, la complexité du problème et des analyses qui en découlaient, ne permettaient pas à des profils peu initiés à la commutation, aux équipements et fonctionnalités associés de pouvoir expliquer simplement et répondre aux questions que pouvaient se poser le management, principalement celui du client. Ainsi, j'ai dû accompagner l'équipe locale dans toutes les conférences téléphoniques. Cela augmentait beaucoup ma quantité de travail, puisque je devais assurer plusieurs conférences par jours.

J'aurai pu refuser de participer à ces conférences téléphoniques, mais je ne l'ai pas fait pour les raisons suivantes. Cela faisait déjà plusieurs jours que je travaillais en étroite collaboration avec l'équipes locale et une relation de confiance s'était mise en place. Cette relation facilitait la communication et les conseils que je promulguais étaient pris au sérieux. Aussi, pour le client il était préférable de garder les mêmes intervenants dans les réunions téléphoniques. Une autre raison était que l'ingénieur N3 et moi ayant une confiance réciproque, celui-ci savait qu'il pouvait me laisser réaliser la plupart de la communication vers l'équipe locale et le client, cela lui permettait de se dégager plus de temps soit pour travailler sur l'appel ou sur d'autres appels critiques qu'il avait à gérer simultanément. Enfin, pour des raisons de gestion du décalage horaire, il était aussi plus facile que je pilote la communication technique, le client se trouvant en Europe.

La figure qui suit représente l'emploi du temps liée aux conférences téléphoniques durant une journée type lors de l'escalade. Il est évident qu'une grande partie de mes journées étaient donc occupées par la communication pour expliquer l'avancement de la résolution du problème et des analyses techniques. Ce qui m'obligeait à travailler très vite et presque sans discontinuer en parallèle sur la partie technique. C'est aussi l'une des raisons pour laquelle cette escalade a été particulièrement intensive de mon côté.

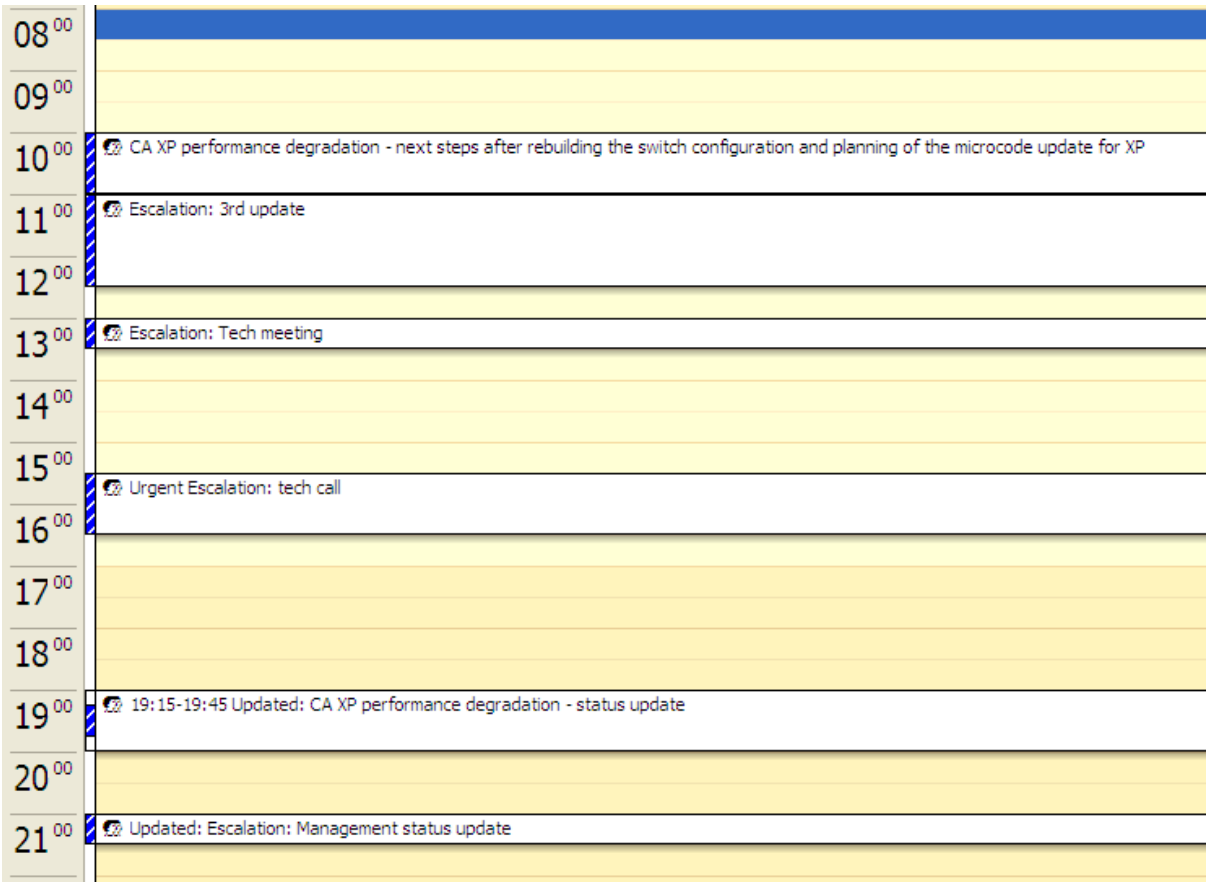


Figure 31: Emploi du temps d'une journée type lors de l'escalade.

Enfin, on peut se poser la question si toutes ces responsabilités et cette charge de travail étaient réellement liées à mon rôle. De mon point de vue, j'ai réalisé ce que l'on attendait de moi, même si j'ai à plusieurs reprises alerté ma hiérarchie sur les dérives de ce qui m'était demandé de faire. Quoi qu'il en soit, je sais depuis, que mon travail a servi et qu'il a été apprécié à juste titre, aussi bien par le client, ma hiérarchie que par les collègues de mon équipe et de l'ingénierie.

Néanmoins, si je devais être impliqué à nouveau dans une escalade similaire, je saurai probablement mieux appréhender le travail à fournir. Je définirai mieux les limites de mon rôle et de mes responsabilités en rapprochant, s'il le faut, mon manager à l'équipe d'escalade afin d'avoir une meilleure répartition des tâches. Ce dernier point est très important, car accepter une tache qui ne nous incombe pas peut s'avérer très pénalisant durant la gestion d'un appel. On peut se retrouver en difficultés, pour des raisons d'accès aux informations ou de compétence, pour mener à bien une action qui nous est demandé de faire. Il est donc important que les acteurs soient clairement identifiés et que la répartition des taches corresponde aux profils et métiers de chaque intervenants.

8.2. Analyses de la réactivité et des plans d'actions

► Réactivité lors de la prise de l'appel.

Même si le problème n'a pas été élevé de façon critique au début de l'appel, il a quand même été traité dans les temps. Une des caractéristiques du travail du support de Niveau 2 consiste

en l'étude d'un problème quelconque en profondeur, afin de fournir une analyse précise. Ainsi, ayant suffisamment de temps dès le début de cet appel pour travailler sur l'analyse, il a été immédiatement possible de fournir un support de qualité mené avec diligence même si l'appel n'avait pas été élevé avec une criticité haute. Pourtant si dans mon équipe nous avions été dans une période où les ressources de personnels avaient été plus réduites où si nous avions déjà été pris par une charge de travail importante, alors, il est tout à fait possible que ce problème aurait attendu.

Il est donc important que le travail réalisé lors de la création de l'appel soit fait de façon précise et que le problème soit bien compris par les différentes parties, y compris la définition faite par le client. Ce sont ces premiers points qui permettent ou non une excellente réactivité.

Il est tout aussi primordial de permettre aux équipes de deuxième et troisième niveau d'avoir une charge de travail adaptée afin d'avoir la possibilité de s'immerger totalement dans un appel. Ainsi, les objectifs du management de ces équipes s'orientent plus vers une approche qualitative que quantitative sinon il ne serait pas possible de maintenir ce niveau de service et donc de procurer une haute valeur ajouter à la gestion technique des appels.

► Gestion de l'influence du management lors des premières phases de l'analyse.

Dans la situation que nous avons rencontré, il y avait une très forte pression du management, autant HP que client, afin de résoudre le défaut au plus vite. Il faut donc être capable de fournir une analyse et les actions associées dans des délais très courts. Le premier aspect d'un plan d'actions est de fournir une liste d'étapes et d'opérations afin de mieux définir le problème ou au mieux de le corriger. Mais, un autre aspect est la communication au niveau managériale. Lors d'une très haute escalade, il est possible d'avoir des conférences téléphoniques plusieurs fois par jours afin de notifier à tous les intervenants l'état d'avancement de l'analyse. Ainsi, on doit être capable de montrer aussi bien au client qu'en interne chez HP, que le travail progresse et que des actions sont en cours. Toutefois, certaines analyses peuvent être longues avant de pouvoir réellement fournir un premier plan d'actions qui ait du sens, ceci peut être dû à plusieurs facteurs, comme la taille des logs à analyser, des informations contradictoires sur le comportement ou bien des informations imprécises. Ces différents facteurs sont forcément défavorables lorsque l'on doit aller vite dans l'analyse.

Ainsi, un paradoxe peut se créer. Car il nous est demandé de fournir une analyse dans des délais très courts, alors qu'il n'est pas possible de fournir des informations pertinentes en si peu de temps. Comme il n'y a pas réellement de solution à ce dilemme, il est donc essentiel d'être capable de trouver le compromis entre le travail technique et la communication. Autrement dit, être capable de faire avancer l'appel correctement tout en gardant en priorité la pertinence technique mais en même temps en permettant au management une communication prouvant de l'avancement du travail en cours et de l'efficacité des plans d'actions.

► Réflexion sur la pertinence des actions.

Une fois le problème résolu, sa source parait évidente et je pense maintenant qu'il aurait peut-être été possible de corriger le problème plus rapidement. Toutefois, je reste convaincu que mon approche a été la bonne. Il fallait bien en premier lieu stabiliser l'environnement et le

faire de façon cohérente et suffisamment professionnelle afin de ne pas perturber le reste du trafic. Ainsi, est-ce que la mise en place des actions liées à l'analyse des instabilités des ports de baies ou au test de la commande "ping" étaient-elles réellement essentielle à ce stade de l'appel ? Probablement. Mais les compteurs des interfaces TCP pouvaient certainement me fournir déjà les bonnes indications sur le problème. Evidemment, aujourd'hui, je peux le confirmer, mais en même temps au moment de l'appel, rien ne pouvait présager que cette infrastructure pouvait être la source du problème.

En effet, l'équipe qui avait installé l'infrastructure maintenait qu'il avait été possible d'obtenir des performances proches de 350 Mbps lors des phases de recette [33] avec le client. En même temps, le client, quant à lui, maintenait que son infrastructure réseau n'avait subit aucune modification et était toujours aussi stable et performante. Nous avions donc, la confirmation que l'infrastructure était capable d'atteindre les performances escomptées et qu'il n'y avait pas eu de modifications récentes, alors que nous pensions que le problème pouvait venir quand même d'un défaut lié au réseau.

De ce fait, et par expérience, le meilleur moyen de résoudre ces problèmes de performance est de commencer l'analyse en tentant de réduire l'environnement. Comme je l'ai évoqué dans la partie liée aux améliorations, il est extrêmement difficile de définir quel est l'élément qui limite les performances. Ainsi, je pense que le travail fourni pendant l'analyse n'était pas vint et que ces différentes étapes nous ont permis d'accomplir le travail qui consistait à réduire le nombre d'éléments pouvant perturber l'infrastructure.

► Implication des autres équipes.

Une tache importante du travail d'ingénieur support est de savoir trier et synthétiser les informations afin de corriger un problème ou de pouvoir faire appel à d'autres équipes, le cas échéant. A mon niveau, ces autres équipes sont généralement l'Ingénierie aux Etats-Unis ou le support constructeur, mais il peut aussi s'agir d'une équipe de niveau 2 relative à une autre spécialité ou technologie. Il faut dans ce cas, être capable de regrouper les informations importantes afin de pouvoir intégrer ces équipes au mieux pour ne pas reperdre du temps dans les phases initiales de leur travail. Ainsi, je pense que j'ai su impliquer les équipes d'Ingénierie HP et support Cisco au moment le plus opportun. Il en va de même pour l'implication du support réseau Niveau 2. En effet, ayant été impliqué dans l'appel alors que le problème n'était pas bien identifié, il aurait été encore plus compliqué de travailler avec d'autres équipes, j'ai ainsi pu mieux identifier les zones d'ombres, les interrogations et les aspects qui me paraissaient les plus pertinents afin d'utiliser au mieux l'expertise de mes homologues. Ainsi, il a été possible de faire évoluer les plans d'actions de manière cohérente et d'orienter l'analyse du problème de façon logique et professionnelle.

Il y a encore quelques mois, les processus internes du support HP nécessitaient l'ouverture de d'appel entre les N2 par l'intermédiaire du support de premier niveau. Aujourd'hui, il existe un nouveau processus qui nous permet de contacter officiellement les ingénieurs de niveau 2 de n'importe quelle équipe afin de les impliquer dans un appel, ce qui améliore la réactivité dans la gestion.

[33] Recette : Protocole de test mené, en fin de projet et en présence du client, afin de confirmer que l'infrastructure installée correspond au cahier des charges.

► Gestion du stress et de la fatigue.

Une des difficultés lorsque l'on travail sur de tels appels est la gestion du stress et de la fatigue. En effet, il a fallu pour les intervenants travailler près de 18h par jours les trois premiers jours de l'escalade. Ainsi, il faut être capable de maintenir l'effort sur une longue période.

De plus, n'étant pas supposé être en astreinte dédiée pour ce problème, il était tout à fait possible que je sois contacté pour un autre appel tout aussi urgent lors de mon astreinte. Cela pouvait être très problématique, car je ne pouvais pas refuser de travailler sur un nouvel appel. Ainsi, mon management, a fait en sorte de pouvoir impliquer l'équipe homologue pour la partie Amérique et utiliser le décalage horaire pour être sûr que cette équipe puisse accepter tout nouvel appel d'astreinte supplémentaire. Il était d'autant plus facile de le faire, puisque certains des ingénieurs qui composent cette équipe sont basés sur la côte Ouest des Etats-Unis. Ainsi, avec 9h de décalage horaire la plus grande partie de ma nuit d'astreinte pouvait être couverte.

Ce type d'approche pour couvrir les astreintes, appelé Follow The Sun (FTS), est déjà formalisé dans d'autres équipes. Les appels d'astreinte d'une zone géographique donnée (APJ, EMEA ou AM) sont pris durant le travail en heures ouvrées par une équipe d'une autre zone géographique. Le principal problème pour la mise en place de ce type de procédé est qu'il nécessite des équipes similaires en nombre et en compétences sur les trois zones géographiques, et que tous les processus soient harmonisés. Ce procédé est en cours de mise en place pour ma technologie et ce fut la première fois que l'on travaillait de cette façon.

PARTIE C – CONCLUSIONS

9. Conclusion

9.1. Conclusion technique de cet appel.

A l'issue de l'appel, il n'a pas été possible de pointer un unique défaut ou source du défaut dans l'infrastructure qui aurait pu être à l'origine de la perturbation, car ce type d'environnement est très complexe et particulier. Il semble que l'origine du défaut soit due à un ensemble de facteurs aggravants et concomitants, qui mis ensemble ont généré le problème de réplication. Ces facteurs peuvent être identifiés comme suit:

► Une augmentation de la quantité de données à répliquer.

Une semaine avant l'apparition du problème, le 12 mars 2008, il y a eu une augmentation des données à répliquer d'environ 1To. Cet événement peut être définit comme le point de déclanchement du problème. La configuration de l'infrastructure telle qu'elle était avant la résolution de l'appel, ne pouvait accepter cette augmentation. Ceci était dû au fait que les performances avaient déjà atteint leurs limites.

► Une anomalie logicielle des commutateurs MDS.

Depuis le mois d'août 2007, les commutateurs rencontraient le problème de déconnexions intempestives des tunnels TCP dû au bug décrit dans ce mémoire. Ces interruptions étant aléatoires, il y avait toujours au moins 2 ou 3 tunnels actifs simultanément. Cela dégradait les performances, mais la quantité de données à répliquer pouvait supporter ces déconnexions, même si l'infrastructure devait sûrement être à ses limites. Suite à la nouvelle augmentation des données à répliquer, les coupures de ce type furent bien plus "visibles" et pénalisantes. Il est à noter que le client avait commencé à remonter le problème de performance en interne à la date du 12 Mars 2008 et que ce jour-là, il y avait eu une augmentation de données mais aussi des ruptures de liens TCP.

► Une mauvaise configuration des paramètres TCP.

Les profils FCIP qui définissent les caractéristiques des tunnels TCP n'étaient pas bien configurés. Le risque était de saturer les liens STM1 et ainsi de créer les conditions de retransmissions de paquets et de la non utilisation optimale de la bande passante. Ces mauvaises configurations qui amenaient donc à des performances dégradées étaient les valeurs maximum de la bande passante et du RTT. Pour ce dernier, il y avait eu une déviation de la latence amenant à une mauvaise optimisation de la bande passante et des risques de saturations.

► Une transmission sur plusieurs chemins physiques avec des latences aléatoires.

Enfin, l'utilisation de plusieurs chemins physiques présentant des temps de latences différents et aléatoires était le facteur probablement le plus aggravant. En effet, même si le réseau du client respectait les spécifications d'origine convenues avec le fournisseur, il y a eu à la période du défaut une fluctuation de la latence de certains liens, ce qui amenait inévitablement

à des réceptions de paquets dans le désordre et donc de retransmissions. Ce phénomène a été mis en exergue par l'augmentation de la volumétrie à répliquer. Ainsi, la modification de l'infrastructure permet depuis d'être préservée de ces fluctuations de latences.

9.2. Conclusion sur ce que m'a apporté cet appel.

Cet appel m'a été bénéfique pour plusieurs raisons. Il m'a permis de confirmer plusieurs aspects de mon travail. Les connaissances techniques ne suffisent pas toujours. Il faut savoir aussi, bien accompagner et rassurer quant à l'analyse et l'avancement du travail, ce qui permet une meilleure visibilité pour le client. Ainsi, lorsque les intervenants sont en confiance, il est plus aisé de travailler sereinement. Je déclinerai ma conclusion sur quatre aspects différents de ce que m'a apporté cet appel.

► Se prouver de ce dont on est capable

Il m'arrive de douter parfois de mes compétences, de mon aptitude à fournir une analyse technique pertinente. Travailler sur ce type d'appel est très éprouvant, mais permet de prouver sa place au sein d'une équipe d'experts. Ainsi, il est certain que suite à cet appel, j'ai eu une toute autre perception de mon travail personnel et de ma légitimité au sein de mon équipe. De même, la considération de mon manager direct et celle de mes collègues de travail ont été elles aussi augmentées.

► Montrer la compétence de mon équipe à travers mon travail

Dans nos organisations, la plupart des relations entre les équipes se font au travers d'outils informatiques, il y a donc peu, voire pas du tout, de contacts physiques entre les personnes. Il est donc important de pouvoir améliorer ces relations, puisque le risque au travers de ce type de contacts "virtuels" est de voir des préjugés ou a priori s'installer. Ainsi, avoir l'opportunité de travailler avec plusieurs équipes dans des situations difficiles permet de prouver la compétence de notre équipe. Il est certain que si mon travail avait été médiocre, l'impression donnée au sujet de mon équipe aurait, elle aussi, été mauvaise.

► Montrer à sa hiérarchie ce dont on est capable

Dans mon métier, au quotidien, je gère des appels. Ils peuvent être plus ou moins techniques, avec plus ou moins de criticité. Lors de la gestion des appels, il y a différents marqueurs et processus qui permettent de noter et d'évaluer notre efficacité, toutefois la valeur ajoutée que l'on a, lors de la gestion d'un appel, n'est pas toujours évidente à mesurer. Ainsi, cette participation à un appel aussi important, avec une très forte visibilité interne à l'entreprise HP, m'a permis de montrer à ma hiérarchie la valeur réelle de mon travail et de mes compétences. Dans le cadre de cet appel, je sais que mon travail a été extrêmement apprécié par ma hiérarchie jusqu'au niveau de management élevé. Cette appréciation m'a été démontrée par l'intermédiaire de ce qui s'appelle des eAwards, qui sont des primes exceptionnelles récompensant un ingénieur lorsqu'il a fait un travail exemplaire. Le premier m'a été donné, à titre individuel, par mon manager de deuxième niveau, le second, a été donné à titre collectif (à tous les intervenants HP de l'appel), par le management supérieur. Par le biais de cet appel,

j'ai confirmé à mon supérieur hiérarchique ma pertinence technique, ma compétence lors de la gestion d'appels complexes et aussi ma capacité à travailler en équipe, de manière soutenue. C'est, entre autres, suite à cet appel qu'il m' a considéré comme un des leaders de l'équipe.

► Montrer à un client ce dont est capable une organisation support.

L'un des points le plus important, à mes yeux, est la capacité de confirmer les choix d'un client dans le fournisseur de services qu'il a sélectionné. En effet, l'organisation support est la dernière organisation à travailler avec le client. Il y a eu auparavant, dans la plupart des cas, les équipes d'avant-vente pour la réponse à l'appel d'offre, puis les équipes projets pour le déploiement de la solution. Enfin, nous sommes les derniers à maintenir la relation client-fournisseur. Par le biais de cet appel, le client a pu se rendre compte de l'efficacité de notre travail au travers de notre réactivité, de notre haute technicité, de notre disponibilité pour résoudre au plus vite la crise.

Il est important de mettre en avant le fait que les clients ou les équipes qui font appel au support ont parfois du mal à travailler avec des relations "virtuelles", et qu'il y a une méfiance quant à l'implication des personnes ou même quant à leurs compétences. Ceci est dû, entre autres, aux processus qui peuvent être non transparents pour le client et à la mauvaise image de l'off-shoring[34] dans l'opinion, déteignant sur celle du travail à distance. Il est donc primordial de prouver aux clients notre réelle compétence par l'assistance que nous prodiguons lors d'appels de ce type.

9.3. Conclusion sur ce que m’a apporté le cursus IDPE

Je sais que le cursus IDPE m'a d'ores et déjà apporté énormément quant à l'approche que j'ai de mon travail au quotidien. En effet, avant d'entamer ce cursus je faisais parfois certaines actions de façon intuitive, sans forcément prendre le recul nécessaire afin de me demander dans quelle démarche elles s'inscrivaient. La rédaction de ce mémoire m'a permis de mieux décomposer mon travail, en mettant en avant les qualités essentielles qu'il faut pour mener à bien mon rôle d'ingénieur. Ainsi, j'ai aujourd'hui la certitude que les qualités telles que la compétence technique, la pertinence, la créativité et la capacité à négocier ne peuvent être dissociées de la qualité d'un ingénieur. Et je suis parfois impliqué dans des escalades où ma partie technique n'est plus en question mais où je continue d'être force de proposition.

Ainsi, de mon point de vue, s'inscrire dans la démarche du cursus IDPE, c'est avoir la maturité professionnelle suffisante pour s'interroger sur le travail accompli depuis plusieurs années ; c'est l'opportunité de regarder dans sa pratique passée en se questionnant sur les réussites et les échecs et en même temps, de se projeter dans l'avenir en se demandant vers quels objectifs professionnels tendre.

10. Bibliographie

► Internet Engineering Task Force (IETF):

rfc793: Transmission Control Protocol, protocol Specification, septembre 1981.

fc2581: TCP congestion control, avril 1999.

rfc3173: IP Payload Compression Protocol, septembre 2001.

rfc3821: Fibre Channel over TCP/IP, juillet 2004.

► American National Standard Institute (ANSI):

FC-FS: Fibre Channel - Framing and signalling, revision 1.90, avril 2003.

FC-PI-2: Fibre Channel - Physical Interface, revision 10.0, aout 2005.

► Documentation Cisco:

Cisco MDS9000 Family CLI configuration guide, Release 3.x, février 2007.

Cisco MDS9000 Family Cookbook for Cisco MDS SAN-OS release 3.1, Seth Mason & Venkat Kirishnamurthyi, octobre 2007.

Cisco Data Center: San Extension for business continuance version 1.2, 2004, Solution Reference Network Design.

Storage Networking Fundamentals, Marc Farley, 2005, Cisco Press.

► Documentation Hewlett-Packard:

San Design Guide 48th Edition, mars 2009, HP StorageWorks.

NES2-SAN-Fundamentals, training material version 2, 2001, HP Workforce & Development.

► Normalisation:

British Standard Institute: Normes BS25999 à propos de la continuité des affaires.

ISO: Normes ISO20000 et ISO27001 à propos de la sécurisation de l'informatique.

11. Glossaire.

A

Accélération: Capacité de réduire le temps des échanges en utilisant le commutateur pour simuler les messages du récepteur final. Voir Write-Acceleration (WA)

ACK (Acknowledgement): L'aquittement est un message envoyé par le récepteur afin de notifier le transmetteur que les paquets ont bien été reçus.

AM (America): Zone géographique regroupant l'Amérique du Nord, l'Amérique centrale et l'Amérique du sud.

APJ (Asia Pacific & Japan): Zone géographique regroupant les pays d'Asie, de l'Océanie et du Japon.

ASIC (Application Specific Integrated Circuit): Composant électronique évolué intégrant des fonctionnalités définies.

B

B2B (Buffer to Buffer Credit): Acronyme utilisé pour désigner la mémoire tampon d'une interface FC.

Backup: Terme anglais qui désigne la sauvegarde des données.

Bug: Terme anglais pour définir une anomalie logicielle.

C

CA (Continous Access): Technologie HP pour permettre les copies directement entre les baies de stockage

Compression: Capacité de réduire la taille d'une trame en utilisant des algorithmes de calculs mathématiques.

Core-Edge: "Core" signifie "cœur" dans le sens d'équipement centralisé et "Edge", signifie "bord", dans le sens d'équipement d'extrémités.

CRC (Cyclic Redundancy Check): contrôle de redondance cyclique, fonctionnalité intégrée au protocole Ethernet pour vérifier l'intégrité d'une trame.

D

Delta: Comparaison de deux logs identiques capturés à deux moments différents afin de voir l'évolution des erreurs.

Direct Attach (attachement direct): Terme anglais qui définit un serveur qui accède à un ou plusieurs équipements de stockage directement connectés.

DR (Disaster Recovery): un site DR, est un site distant du site principal permettant le redémarrage des activités en cas de sinistre informatique.

DRP (Disaster Recovery Process): Procédures à mettre en place lors d'un sinistre informatique afin de rétablir les applications.

Dual-Fabric (Double Fabric): Utilisation de deux fabrics composées à l'identique afin de créer une redondance.

E

E_D_TOV (Error Detect TimeOut Value): Compteur utilisé pour détecter une erreur dans la durée de transmission de messages de contrôle. La valeur par défaut est 2000ms.

Edge: Equipement d'extrémité dans une topologie Core-Edge.

Elévation: Processus dans l'organisation support qui permet d'impliquer un niveau de support supérieur afin d'assister l'analyse technique.

EMEA (Europe Middle East and Africa): Zone géographique comprenant les pays d'Europe, du Moyen-Orient et de l'Afrique.

Encapsulation: Mécanisme qui permet d'intégrer une trame d'un protocole différent.

Escalade: Processus, dans l'organisation support, qui permet d'impliquer le management dans la gestion de l'appel et la relation avec le client. Utilisé dans les cas graves.

F

FC (Fibre Channel): Protocole utilisé dans le monde du stockage.

FCIP (Fibre Channel over Internet Protocol): Encapsulation du protocole FC dans le protocole IP afin d'utiliser l'infrastructure réseau pour transmettre les données du SAN.

Firmware: Terme anglais qui désigne le logiciel ou microcode d'un équipement.

G

GigE (Gigabit Ethernet): Interface qui permet la connexion d'équipements communiquant avec le protocole Ethernet.

H

HBA (Host Bus Adaptor): Carte présente dans le serveur comportant les éléments (Asic, connecteurs, …) pour la connexion aux équipements extérieurs.

I

ICMP (Internet Control Message Protocol): Protocole de la 3ème couche OSI (comme le protocole IP) utilisé pour les messages de contrôle et d'erreurs.

IPComp (IP Payload Compression Protocol) – aussi appelé IPPCP: En-tête contenant les informations liées aux données compressées.

IVR (Inter Vsan Routing): Possibilité de faire communiquer des équipements dans des VSAN différents.

J

Jumbo frame: Trame « géante » permettant un MTU supérieur à 1500 Octets.

L

LAN (Local Area Network): Réseau couvrant des distances relativement faibles et associé au matériel permettant la communication entre les équipements.

Latence: Temps de propagation du signal au travers de l'infrastructure.

Logs: Génération des messages d'erreurs, des événements, compteurs d'erreurs,… d'un équipement.

M

MDS (Multilayer Datacenter Switch): Gamme de commutateurs Fibre Channel du constructeur Cisco.

MTU (Maximum Transfer Unit): Taille maximale des trames Ethernet sur le réseau.

O

Off-shore: délocalisation des compétences vers les pays à faible coût.

On-shore: pays à fort coût, en opposition aux pays Off-shore.

Out Of Order: Réception de trames dans le désordre.

P

Ping: Commande utilisant le protocole ICMP pour contrôler la communication entre deux équipements réseau.

Port-channel: Agrégation de plusieurs liens physiques en un seul lien logique.

Q

QoS (Quality Of Service): Capacité à faire de la qualité de service en distinguant les différents types de trafic et en leur attribuant des priorités différentes.

R

R_RDY (Receiver Ready): Message de contrôle qui permet de prévenir le transmetteur que le récepteur a un nouveau buffer de disponible.

Recette: Protocole de test mené, en fin de projet et en présence du client, afin de confirmer que l'infrastructure installée correspond au cahier des charges.

Redondance: Notion qui dédouble le matériel dans l'infrastructure afin d'être plus tolérant aux pannes.

Release Notes: Documents officiels constructeurs informant des nouveautés, modifications, corrections de défauts apportées dans une version logicielle spécifiée.

Réplication : copie des données depuis un site local vers un site distant visant à garantir leur disponibilité en cas de sinistre informatique.

RPO (Recovery Point Objective): Quantité acceptable de données perdues depuis la dernière sauvegarde

RTO (Recovery Time Objective): Temps maximal qu'il faudrait pour le rétablissement des applications en cas de sinistre informatique

RTT (Round Trip Time): Temps que met un paquet à aller et revenir d'un point à l'autre du réseau.

S

SAN : (Storage Area Network) réseau haut débit dédié au stockage.

SCSI (Small Computer System Interface): Protocole de couche haute définissant l'échange de données entre un émetteur et un récepteur dans le stockage.

SDH (Synchronous Digital Hierarchy): Protocole de transmission des opérateurs télécom généralement utilisé dans les infrastructures longues distances à haut débit.

Segmentation : terme signifiant que la liaison entre deux commutateurs FC est interrompue.

STM1 (Synchronous Transport Module – 1): Standard définissant la transmission du protocole SDH avec un débit de 155Mbps.

T

Timeout: Terme anglais définissant le dépassement du temps imparti pour une opération.

Topologie: Disposition logique des éléments composant le réseau et de leurs interconnexions.

Trame: Ensemble de bits représentant le message à transmettre.

U

Upgrade: Terme anglais signifiant la mise à niveau logicielle d'un équipement.

V

VSAN (Virtual SAN): Possibilité de fragmenter un SAN de façon logique.

W

WA (Write Accélération): Accélération en écriture.

WAN (Wide Area Network): Réseau informatique regroupant les matériels sur une grande distance.

X

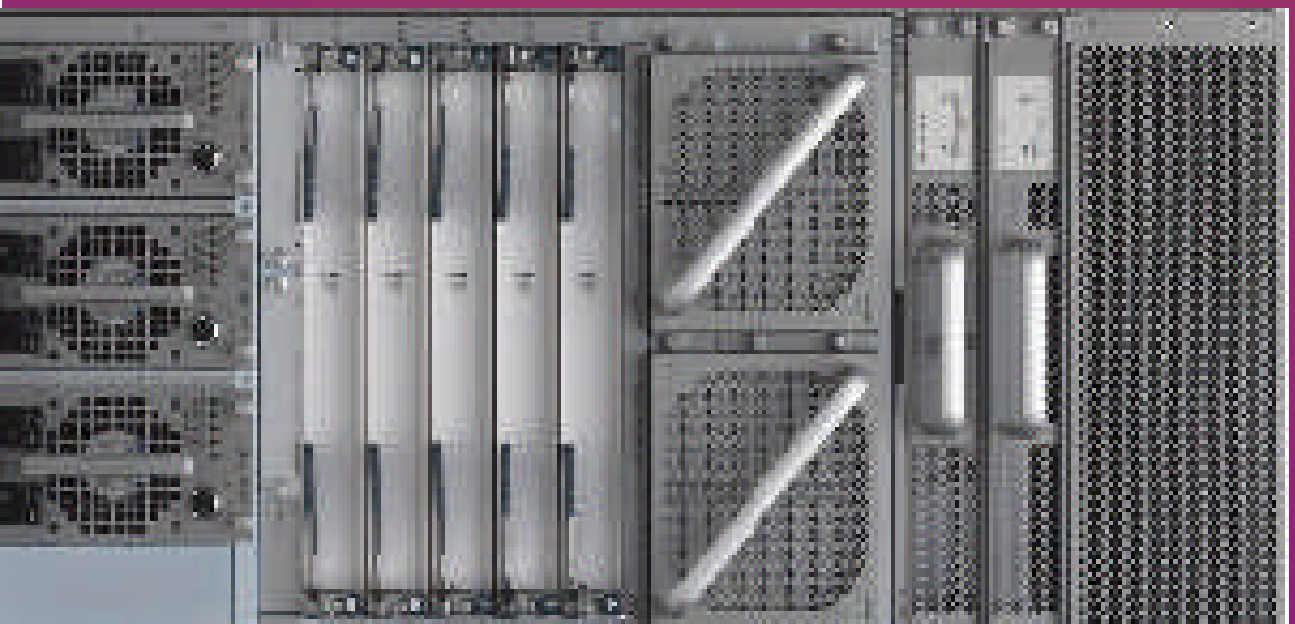
XP12000: Modèle de baies de stockage du constructeur HP.

Workaround: Solution de contournement afin de ne pas rentrer dans le périmètre d'un bug.

Z

Zoning: Notion de cloisonnement dans un SAN permettant de sécuriser la communication en créant des associations d'équipements autorisés à communiquer entre eux.

PARTIE D – ANNEXES



12. Annexes

12.1 Annexe 1 : Rapport d'escalade officiel au 23 Mars 2008

	Formal Escalation Report	
	Customer Data replication problem	

1. General Information

Start Date:	3/19/2008 4:16:12 PM
Status:	open
Category:	Regional Esc.
Origin:	Incident Mgmt./Incident
Detailed Status:	Data replication between two XP 12000 is suspended
Trigger:	High Business Impact
Escalated By:	Account Support Team
Escalation Type:	TS Value SWD
Customer Region:	EMEA
Service/Service Level:	MC BCS
Product/Issue Category:	Hardware
Product/Issue Sub-Categ.:	SAN/Mass Storage Interconnect
Possible Root Cause:	Not determined
Support Organization:	Solution Center
Support Region:	EMEA
Support Sub-Region:	CEE

2. Detailed Descriptions

Current Situation

The production hasn't been impacted yet but it is still at serious risk because of no disaster recovery for 2 countries.

Short term goal: #1 priority – replicate 3 of 4 countries by Sunday evening
- Country 1 has been fully replicated
- Country 2 has been fully replicated
- Country 3 has been fully replicated
- Countries 4 & 5 is started

HP SAN CC, Cisco TAC, Networking experts together with local technical resources and also together with Csutomer team and ISP provider are splitting the 2 out of 3 STM lines in order to dedicate them to fcip modules from MDS to MDS in order to avoid multipathing that is causing out-of-order packages and retransmitting.

Long term – root cause resolution
- We haven't been able to identify the root cause yet
- However we managed to identified most likely cause is related to SAN MDS Switch and LAN/WAN.
- We also believe that we can exclude both XP's as possible causes for the time being.
- The resolution team has been working on resolution in parallel to running application and with extreme cautious in regards to Customer production
- SAN MDS Switch logs have been collected and Cisco TAC sent them Cisco labs to be analyzed.

Next plan:
- Keep replication of Countries 4 & 5 steady and running till is fully completed
- Review and discuss outcome of SAN MDS Switch logs that are being to be analyzed by Cisco labs
- Internal touch points are also scheduled for Sunday

	Formal Escalation Report	
	Customer Data replication problem	

Initial Situation
Customer bank's data are not replicated to disaster site for some countries.

Customer Business Impact
critical Customer business impact is that currently the BANK's data are not replicated to DR site.

Closure Criteria
Successfull data replication restored within customer's time expectations.

Communication Plan
EMO: HP customer Management <> Customer IT Infrastructure Manager HP country management <> Customer Management Team Technical Team ASM: Customer support management <> HP Management & customer management

3. Actions

Action 1.0	
Title:	Initial Assessment
Owner:	Customer account manager
Status:	closed
Due Date:	3/19/2008 6:00:00 PM
On March 18th Customer Reported data replication problem. Standby Engineer was informed that replication sessions for some countries were suspended and replication for Country 4 data was very slow. Standby engineer went on site and examined the condition of the XP storage and MDS CISCO switches and found no H/W issues. He collected the relevant logs and elevated the case to Storage Competency Centre for further investigation.	

Action 2.0	
Title:	Provide the matrix of the replication per country
Owner:	Customer account manager
Status:	closed
Due Date:	3/19/2008 8:30:00 PM
Create a table stating for which countries the data replication is OK, for which countries the data replication has slow performance, and for which countries the data replication is suspended. Countries 1 a 2 impacted	

Action 3.0	
Title:	Inform the custmer about the escalation
Owner:	Customer Service manager
Status:	closed
Due Date:	3/19/2008 10:30:00 PM
The customer will be informed about the escalation. The communication will include the action plan, the closure criteria and the communication schedule.	

	Formal Escalation Report	
	Customer Data replication problem	

Action 4.0	
Title:	ensure that required data are provided to STC by local team
Owner:	Customer account manager
Status:	closed
Due Date:	3/19/2008 10:15:00 PM
The information was sent via e-mail by local team, but must to be uploaded also to WFM. provide nd dump or better link where all dumps are located	

Action 5.0	
Title:	Provide historical data of known changes of XP12000 to HP Support organization as appropriate
Owner:	Customer account manager
Status:	open
Due Date:	3/26/2008 12:00:00 PM
We have information about changes related to Tuesday when the first incident was happen. We still to dot have information about the changes before that.	

Action 6.0	
Title:	Conf call for status update at 22:00 EET (first)
Owner:	Customer Service manager
Status:	closed
Due Date:	3/20/2008 12:00:00 AM
In the conf call will be presented the status of the current situation.	

Action 7.0	
Title:	Conf call for status update at 12:00 EET (second)
Owner:	Customer Service manager
Status:	closed
Due Date:	3/20/2008 2:00:00 PM
The second conf call for status update	

Action 8.0	
Title:	Define the technical action plan
Owner:	Technical Engineer local team site 1 & 2
Status:	closed
Due Date:	3/20/2008 8:00:00 PM
The technical plan will be defined by the technical persons based on the recommendation provided by STC and MCC.	

Action 9.0	
Title:	Send topology of environment
Owner:	Customer account manager
Status:	closed
Due Date:	3/20/2008 1:00:00 AM
Customer support Manager sent data to L3 XP support	

	Formal Escalation Report	
	Customer Data replication problem	

Action 11.0	
Title:	XP troubleshooting
Owner:	XP Engineering expert
Status:	open
Due Date:	3/23/2008 9:00:00 AM
All dumps has been analyzed and there was the recommendation to upgrade the microcode. It is not related to the root cause but it must to be done.	

Action 11.1	
Title:	Provide detailed XP dump from site 1
Owner:	XP Specialist local team
Status:	closed
Due Date:	3/20/2008 4:15:00 AM

Action 11.2	
Title:	Provide detailed XP dump from site 2
Owner:	Technical Engineer local team site 1 & 2
Status:	closed
Due Date:	3/20/2008 1:15:00 AM
the dump was uploaded / provided to L3 XP engineer	

Action 11.4	
Title:	Gerald should do a proper hand over to his successor (Jay?)
Owner:	XP Engineering expert
Status:	closed
Due Date:	3/20/2008 5:00:00 AM
hand over was succesful	

Action 11.5	
Title:	XP L3 should update XP L2 from STC EMEA in the morning
Owner:	Customer Service manager
Status:	closed
Due Date:	3/20/2008 11:00:00 AM
Owner make sure that it will happen	

Action 11.6	
Title:	upgrade XP ucode on both sites (must be schedule)
Owner:	
Status:	pending
Due Date:	
We have to schedule this microcode update.	

	Formal Escalation Report	
	Customer Data replication problem	

Action 11.7	
Title:	create compatibility matrix in regards to microcode upgrade
Owner:	Customer account manager
Status:	open
Due Date:	4/1/2008 2:00:00 PM
XP Microcode update can be done independently but we have to make sure that will not affect all the SAN (all other firmware's and drivers)	

Action 11.8	
Title:	set CAJ on all journal groups bandwith settings to 100Mbps on both XPs (GR-RO)
Owner:	XP Specialist local team
Status:	closed
Due Date:	3/21/2008 5:00:00 PM
simple and clean configuration – L3 XP engineer can help to explain it	

Action 11.9	
Title:	Replace the SFP for port 4K on 23098
Owner:	XP Specialist local team
Status:	closed
Due Date:	3/21/2008 5:00:00 PM
recommended by L3 XP engineer	

Action 11.10	
Title:	Replace the cable for port 4K on 23098
Owner:	XP Specialist local team
Status:	closed
Due Date:	3/21/2008 5:00:00 PM
recommended by L3 XP engineer	

Action 11.11	
Title:	Replace the switch SFP for port 4K on 23098
Owner:	XP Specialist local team
Status:	closed
Due Date:	3/21/2008 5:00:00 PM
recommended by L3 XP engineer	

Action 11.12	
Title:	Send identified XP parts to customer. (Same parts replaced in SEMA)
Owner:	Customer account manager
Status:	closed
Due Date:	3/21/2008 4:30:00 PM
Send identified XP parts to Customer. (Same parts replaced in Site 1) Replace part is sequence and test results after each trial	

	Formal Escalation Report	
	Customer Data replication problem	

Action 11.13	
Title:	XP12000 log analysis
Owner:	XP Engineering expert
Status:	closed
Due Date:	3/21/2008 12:00:00 PM
the log analysis was performed	

Action 12.0	
Title:	Switch back to basic SAN config
Owner:	**Philippe Duboscq**
Status:	close
Due Date:	3/22/2008 11:45:00 PM

Action 13.0	
Title:	Conf call for status update at 24:00
Owner:	Customer Service manager
Status:	closed
Due Date:	3/20/2008 2:00:00 AM
done	

Action 14.0	
Title:	rebuild the SAN to basic configuration - fabric 1 at first
Owner:	**Philippe Duboscq**
Status:	closed
Due Date:	3/20/2008 6:00:00 AM

to avoid any bugs or troubles which could be linked to these features:
So, I would ask to remove the "tcp compression" and "Write acceleration"
Also, from what I have read, the max badwidth between sites is 3x155Mbps= 465Mbps
The rule when we set the Max Bandwidth available per FCIP profiles in the switches is to divide the globale Max bandwidth with the number of FCIP profiles which will go through.
In our case, we have 4 Fcip profiles going through 465Mbps, so the max value per FCIP profile should be 465/4=115Mbps
Then the min value is around 70%, so something like 80Mbps.

The command are the following:
Conf t
Fcip profile X <<enter the value of the configured FCIP profile
tcp max-bandwidth-mbps 115 min-available-bandwidth-mbps 80 round-trip-time-ms 84
Exit

Interface fcip X
no write-accelerator
no ip-compression mode1
Exit

Do the same on each fcip profile for one fabric
If the link flaps again, that means we have another trouble, but at least we will be sure that there are no problem with this config/Firmware.

	Formal Escalation Report	
	Customer Data replication problem	

Action 14.1	
Title:	Reduce traffic (customer & hp)
Owner:	XP Specialist local team
Status:	closed
Due Date:	3/20/2008 5:30:00 AM
together with Lucian and the customer system admins	

Action 14.2	
Title:	rebuild the SAN to basic configuration - fabric 2
Owner:	**Philippe Duboscq**
Status:	closed
Due Date:	3/20/2008 7:30:00 AM

Action 14.3	
Title:	check the performances (the customer & hp)
Owner:	**Philippe Duboscq**
Status:	closed
Due Date:	3/20/2008 9:30:00 AM

the purpose here is to force the MDS switches to not use the full bandwidth, in order to see how the San reacts in term of tcp retransmission… if we see or not retransmission, and at which threshold they appear.

With this method, we are sure that we will fill the ip link with a specific throughput, using the "tcp max-bandwidth" value and this through the MDS.

The advantage of this test is, that it will show us if we have this trouble due to some sort of bandwidth limitation somewhere on MDS or IP network.
And also, if we are able to find a compromise for which no retransmission appear with the highest Bandwidth possible, then we should have a better global throughput over the link.

The problem is, each time we have to make the changes we need to have NO traffic going through the link. Because the FCIP will be down during the parameters changes.
And also, we need to be able to generate traffic after each changes… so stop/start traffic on demand.

The method is the following:
We assum that as yesterday, only traffic will go through 1 fabric (if thorugh 2 fabric we have to divide the value per 2 and do it on all fcip...), so we will do the change only on 2 fcip on 2 switches.
-for both FCIP profile on one MDS on both site: change the tcp max/min bandwidth with the following value:
40/30, 65/50 then 90/70 - if it's too much tests, then we can reduce to 2 tests: 40/30-80/65

Then each time we regenerate traffic, we check the "ips stats for TCP retransmission".
Then, if we are able to see some differences, we can discuss to which value we have to set the Max/min, or if no differences, we will put back to the previous value.

We would start from the bottom, then if retransmission are seen.. Then we can stop the test and go back with the previous settings... That means we will not be able to improve the throughput with this method.

	Formal Escalation Report	
	Customer Data replication problem	

Action 14.4	
Title:	ensure that local HP support team is ready site 1
Owner:	Customer Service manager
Status:	closed
Due Date:	3/20/2008 5:30:00 AM
done	

Action 14.5	
Title:	ensure that local HP support team is ready in Site 2
Owner:	Customer Service manager
Status:	closed
Due Date:	3/20/2008 6:30:00 AM
done	

Action 14.6	
Title:	need new switch logs for all 4 switches by early tomorrow morning
Owner:	XP Specialist local team
Status:	closed
Due Date:	3/20/2008 7:00:00 AM

Action 15.1	
Title:	remove the "tcp compression" and "Write acceleration" on each fabric
Owner:	**Philippe Duboscq**
Status:	closed
Due Date:	3/20/2008 8:00:00 PM
same on each fcip profile for one fabric, and then check the performances.	

Action 15.0	
Title:	provide specific action plan for SAN modification on both sites (2pm EET)
Owner:	**Philippe Duboscq**
Status:	closed
Due Date:	3/20/2008 2:00:00 PM
done and prezented to customer	

Action 16.0	
Title:	arrange conference call together with the customer to discuss action plan for the next evening in details
Owner:	Customer Service manager
Status:	closed
Due Date:	3/20/2008 3:00:00 PM
done	

	Formal Escalation Report	
	Customer Data replication problem	

Action 17.0	
Title:	arrange internal tech meeting with XP and SAN SME inlc ASMs
Owner:	Customer Service manager
Status:	closed
Due Date:	3/20/2008 11:00:00 AM
done	

Action 18.0	
Title:	engage NW CC = open elevation
Owner:	Customer Service manager
Status:	closed
Due Date:	3/20/2008 12:00:00 PM
Owner will make sure that elevation to Network L2 will be opened asap.	

Action 19.0	
Title:	ask the customer to involve 3party network providers
Owner:	Customer account manager
Status:	closed
Due Date:	3/20/2008 1:00:00 PM
local nw specialist + cc network specialist - review networking setup with 3-party network provider	

Action 20.0	
Title:	verify timelines with the customer for maintenance window and touch points
Owner:	Customer account manager
Status:	On going
Due Date:	

Action 21.0	
Title:	install performance advisor (site 1)
Owner:	XP Specialist local team
Status:	pending
Due Date:	

Action 21.1	
Title:	collect and send performance data to XP GCC/STC
Owner:	XP Specialist local team
Status:	close
Due Date:	3/23/2008 12:00:00 PM

Action 22.0	
Title:	Coordinating the investigation of the end-to-end network links condition
Owner:	Customer account manager
Status:	On going

	Formal Escalation Report	
	Customer Data replication problem	

Action 22.1	
Title:	Specify the exact technical information that customer should provide
Owner:	Network Level 2 support expert
Status:	closed
Due Date:	3/21/2008 4:30:00 PM

Action 24.0	
Title:	Provide the detailed reconfiguration (catalyst port mirroring/span)
Owner:	**Philippe Duboscq**
Status:	close
Due Date:	3/23/2008 10:00:00 AM
Provide the detailed reconfiguration (catalyst port mirroring/span) as this proposed by Cisco TAC and kindly presented by Philippe Duboscq	

Action 25.0	
Title:	upgrade FW - MDS Cisco switches
Owner:	**Philippe Duboscq**
Status:	pending
Due Date:	

Action 26.0	
Title:	Common network/SAN/WAN troubleshooting
Owner:	**Philippe Duboscq**
Status:	open
Due Date:	3/23/2008 12:00:00 PM

Based on the Cisco troubleshooting tonight, March 21st, 2008 10:00pm EST, there is evidence of large fluctuations in round-trip-time, rtt, between the routers 7200. The extended ping command was run between the routers which excluded the Cisco MDS switches and resulted in fluctuations of rrt that ranged from 80ms to 168ms. The results also included a substantially high 20% packet loss. At the same time extended rrt was run between the catalysts 6509 and resulted in rrt between 80 and 148 ms. Since the catalysts 6509 sit one hop behind the routers 7200 it is expected the rrt to equal or be larger than 168ms. This is an indication that there is a problem in the network. MDS switches resulted in rtt that ranged between 80ms to 138ms.

Cisco also states that large fluctuation in rrt could have adverse effects on the fcip profiles on the MDS switches which could indirectly contribute to the retransmissions we have been seeing.
We would like the network provider to explain why there are large round-trip-time fluctuations in their OC3 network and why there are substantially high packets lost during XP storage
We would also like the network provider needs to test the network with Cisco and HP present during peak hours of XP storage replication.In the same time, we have to be carefull with any QoS in place we would address different priority depending on the packets type,… which could be a reason of bad ping stats.

	Formal Escalation Report	
	Customer Data replication problem	

Action 26.1	
Title:	extended ping tests to be performed
Owner:	**Philippe Duboscq**
Status:	close
Due Date:	3/22/2008 11:45:00 PM

The IP addresses that were actually used (both source and destination and not just the ones that were assumed to be used).

Please be aware that the routers classify traffic by various criteria (including IP address) and then allocate different bandwidth to different categories. It is quite possible that the ping tests would have been put in a different category than the replication traffic and could therefore have experienced quite different handling within the network. (For example, imagine that the replication traffic is placed in categories A and B but all other traffic goes in category C. If categories A and B are lightly loaded and if replication if performing correctly, then pings may well suffer if category C is overloaded.)

Please also be aware that in all networks that contain service policies it is extremely important to analyse the service policies before you deduce too much from the results of ping tests!!

Title: 26.2	reconfiguration of MDS switches and WAN network equipment
Owner:	**Philippe Duboscq**
Status:	closed
Due Date:	3/22/2008 10:00:00 PM

Following the extensive troubleshooting efforts and the diagnostic testing procedures jointly applied by HP/Cisco Experts (L2/L3/Local Staff), Customer Staff , the HP task force, has reconfigured MDS switches and WAN network equipment in order to definitely eliminate probable contributing factors to the replication issue occurred.

Action 26.3	
Title:	testing the configuration
Owner:	**Philippe Duboscq**
Status:	closed
Due Date:	3/23/2008 2:00:00 AM

After successfully testing the respective configuration - by partially utilizing one STM1 circuit and one logical path with an artificially imposed traffic limitation - the copy operations for Country 4 has been re-initiated, resulting to a full synchronization causing no network errors (e.g. retransmissions & out of order conditions), as previously occurred.

Furthermore, one additional STM1 circuit has been added (totaling 3 logical paths) to the active configuration, resulting to a combined – artificially limited. Additional copy operations have been triggered resulting to flawless synchronization of CM1, CM2 & SE2 groups, as expected.

	Formal Escalation Report	
	Customer Data replication problem	

Action 26.4	
Title:	further optimize the configuration
Owner:	**Philippe Duboscq**
Status:	open
Due Date:	

In order to further optimize the respective configuration, the infrastructure has been parameterized with 2x155Mbps logical paths (supported by 2x STM1) providing total available bandwidth of 310Mbps. The tests performed (SE1 synchronization initiation, error counters examination) have indicated a normal operation/behavior of both the replication and the WAN links, resulting in average transfer rates of 200/225Mbps, causing ZERO "out of order" and "packet retransmission" incidents (07:00).

At the time of writing (Mar. 23 2008 07:30) the replication of the remaining groups is normally progressing … However, there are still pending tasks related to the unbundling of the paired STM1s (owner ISP) and further optimizing the active configuration. (owners HP + Customer)

4.Escalation Team Members

Role Name	**Role description**
HP Management	Customer Service manager
HP Management	Customer account manager
Escalation Specialist	XP Specialist local team
Escalation Specialist	Technical Engineer local team site 1 & 2
HP EMEA L2 Specialist	Philippe Duboscq - San level 2 support expert
HP EMEA L2 Specialist	Network Level 2 support expert
HP WW L3 Specialist	San Engineering expert
HP WW L3 Specialist	XP Engineering expert

Role Name	**Role description**
Esc. Creator	Escalation Initiator – liaise with Esc Mngt
HP Management	Local country HP management
HP Management	EMEA Escalation manager
HP Management	EMEA Escalation manager
HP Management	Customer service manager (local country)
HP Management	EMEA Customer service manager

12.2 Annexe 2 : Procédure d'upgrade.

Part A : Generic recommendations

Part B : Technical actions to be performed before the upgrade

1 – Sanity Check
1.1 – check supervisor flashcard
1.2 – check Moule flashcard

2- Download firmware
2.1 – download kickstart and System firmware
2.2 – download SSi firmware

3- Fabric check
3.1- servers and XP
3.2 – switch check
3.3 – backing up the configuration.

Part C : Technical actions to be during the upgrade

4- Upgrade
4.1 – Switch A
4.2 – Switch B
4.3 – Switch C
4.4 – Switch D

5 – Status check
5.1 – connectivity check
5.2 – application check

6- roll-back
6.1 – downgrade
6.2 – check

Part D : Manual upgrade and troubleshooting commands

6- CLI command to run before
6.1 – check bootflash space
6.1 – copy files
6.2 – check files integrity

7- Manual upgrade

8- Troubleshooting commands

Part A : Generic recommendations

Based on these information, and also based on the fact that the configuration is running old firmware and also that the VC-FC is not supported in the current version,... It might be time now to plan the switch upgrade soon. I keep my recommendation that you need to upgrade first before enabling the WA and Ip-compression.

With the Spock document I have seen, the target SanOS should be 3.2(2c), but, I'm not aware of your full configuration, and you have to check with the current Spock doc which target version is the best or is supported.

I would recommend to do the pre actions, as well as the upgrade itself, on each MDS one at a time fabric per fabric. Then use FM for doing the upgrade or, with CLI, use the command "install all"

Also there are SSM modules, so you need also to upgrade it with the SSI images. BE CAREFULL! The SSM module upgrade is traffic affecting.

You need to do the upgrade while there are no changes in the fabric, and when traffic is the lowest, Just to avoid some troubles. And we would advice you to have few spare modules (sup, LC, ...) just in case.

You can find here the Cisco documentation related to the Firmware upgrade.
http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/san-os/upgrade/guide/upgrade.pdf

3.2(2c) release notes:
http://bali.grc.hp.com/central_san_cc/firmware/release_notes/rn_mds_3.2.2c.pdf

Part B : Technical actions to be performed before the upgrade

1 – Sanity Check
1.1 – check supervisor flashcard
1.1.1 – check the CF card status

http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsi93446&from=summary

To know if any module's CF has an issue detected by OHMS, the syslog can be checked for the above messages with the command

`"show system health statistics module <x>"` like in this example.

```
Bison# show system health statistics module 1
Test statistics for module 1
-------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run     Pass     Fail CFail Errs
-------------------------------------------------------------------------------
Bootflash           Running              10s  1597563 1597563       0     0    0
EOBC                Running               5s  3195126 3195126       0     0    0
Loopback            Running               5s  3194239 3194239       0     0    0
-------------------------------------------------------------------------------
```

1.1.2 – use the script

run the script to check the flash card integrity:

script you could find here, also good explanation how to run it:

http://bali.grc.hp.com/central_san_cc/cisco/cf_card_01.htm

CF Card Failure Document

CF Card Check Up Utility (version 1.0.3 from 05.02.2007)

1.2 – check Module flashcard

check the available flash card memory size, for all modules

```
attach module X   (<< for each module)
dir bootflash:
```

(check for available size, it can be full due to old logs filling the space)

```
show file bootflash:resetscript.log
```

If the command returns an output, and if there is sufficient space on the module bootflash: then the upgrade should go through

2- download firmware

You can find all firmware in our internal website:

http://bali.grc.hp.com/central_san_cc/cisco/firmware_files.htm

Copy the files on a tftp server, then when you will use the FM software install wizard, you will simply have to point this location…

2.1 – download kickstart and System firmware

2.2 – download SSi firmware

Find here the SSI matrix for the SanOS in used.

http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/ssi/compatibility/matrix/SSImtx.html

3- fabric check

The goal here is to confirm before the upgrade that everything is working normally, and that the upgrade can be performed.

3.1- servers and XP

Verify that all servers and XP are all ok, and the dual paths are well working.

3.2 – switch check

Verify that all switches are well working, both CP are redundants, no troubles with interfaces, FCIP, …

3.3 – backing up the configuration.

For each switches, please copy the running config on a tftp server, in order to have a backup of the configuration in case of major troubles.

```
mds9216# copy run tftp:?
  tftp:  Enter URL "tftp:[//server[:port]][/path]"
mds9216# copy run tftp:
```

Part C : Technical actions to be done during the upgrade

4- upgrade

If customer has Fabric Manager, I would advice you to use this software, because most of the commands are automated.
Click either on the icon “software install wizard” or click on “tools/other/software install” and then follow the wizard…

Before doing the upgrade, check if both supervisor are redundants:

```
#Show module
5    0      Supervisor/Fabric-1           DS-X9530-SF1-K9    active *
6    0      Supervisor/Fabric-1           DS-X9530-SF1-K9    ha-standby
```

The upgrade will be done sequencially, switch per switch, fabric per fabric. In order to detect any troubles and to avoid waste of time for any potential roll-back or troubleshooting.

Customer is currently on 3.1(2b) and will go to 3.2(2c) In my opinion customer could run into:
http://www.cisco.com/en/US/products/ps5990/products_field_notice09186a00809398cf.shtml
Under Rare Conditions, a Non-disruptive Upgrade of a DS-C9506, DS-C9509 or DS-C9513 to SAN-OS 3.1(1) through 3.2(2c) or a Subsequent Switchover May Cause the Switch to Reboot - Workaround Provided to avoid the Issue.

4.1 – Switch A upgrade
4.2 – Switch B upgrade
4.3 – Switch C upgrade
4.4 – Switch D upgrade
4.5 – SSM module considerations.

I would like to highlight, that customer uses SSM cards in Site 1:

SSM: Intelligent services traffic on the SSM, such as SANTap, NASB, and FC write acceleration, is disrupted during an upgrade. SSM Fibre Channel traffic is not.

What sort of application is running on SSM modules in Site 1 ?
To which SSI firmware you would like to go on SSM Site 1 ?

5 – status check

5.1 – connectivity check

Verify that all servers and XP are all ok, and the dual paths are well working.

5.2 – application check

Verify that all applications, luns, CA… are well up and running.

6- roll-back

In case of troubles, because you kept the previous Firmware in the switch memory cards, you simply have to do the same task but pointing the previous firmware.

6.1 – downgrade

Use the same method as the upgrade, with FM, but, this time the firmware files are already in the switches memory, so no need to download the files again.

6.2 – check

Part D : Manual upgrade and troubleshooting commands

The goal here is to do the upgrade manually, depending if you are comfortable enough using CLI for this task. The main advantage is that you will follow all the steps and in case of failure or troubleshooting it would be easier to find the root cause.

6- CLI command to run before

6.1 – check bootflash space

With the "dir bootflash:" commands you will see the files already installed and the available space.

The files will have these sizes:

```
Kickstart   :14612 kB
System      :73289 kB
SSI         : 4984 kB
```

6.1 – copy files

Copy the files from a tftp server to the MDS switches:

```
switch# copy tftp://10.16.10.100/system-img bootflash:system-img
switch# copy tftp://10.16.10.100/kickstart-img bootflash:kickstart-img
switch# copy tftp://10.16.10.100/ssi-img bootflash:ssi-img
```

6.2 – check files integrity

The following command will provide you either the Cksum result or the md5 result, these results have to be compared with the data provided in the Cisco website when you downloaded the files.

```
switch# show file bootflash:m9500-sf1ek9-mz.3.0.2.bin.S6 cksum
2427392131
switch# show file bootflash:m9500-sf1ek9-mz.3.0.2.bin.S6 md5sum
4ff0f7b6d6ff60efe5638ac7c3e39128
```

7- manual upgrade

Run the command "install all" commands:

```
switch# install all system bootflash:system-img kickstart
bootflash:kickstart-img ssi bootflash:ssi-img
```

and follow the screen info…

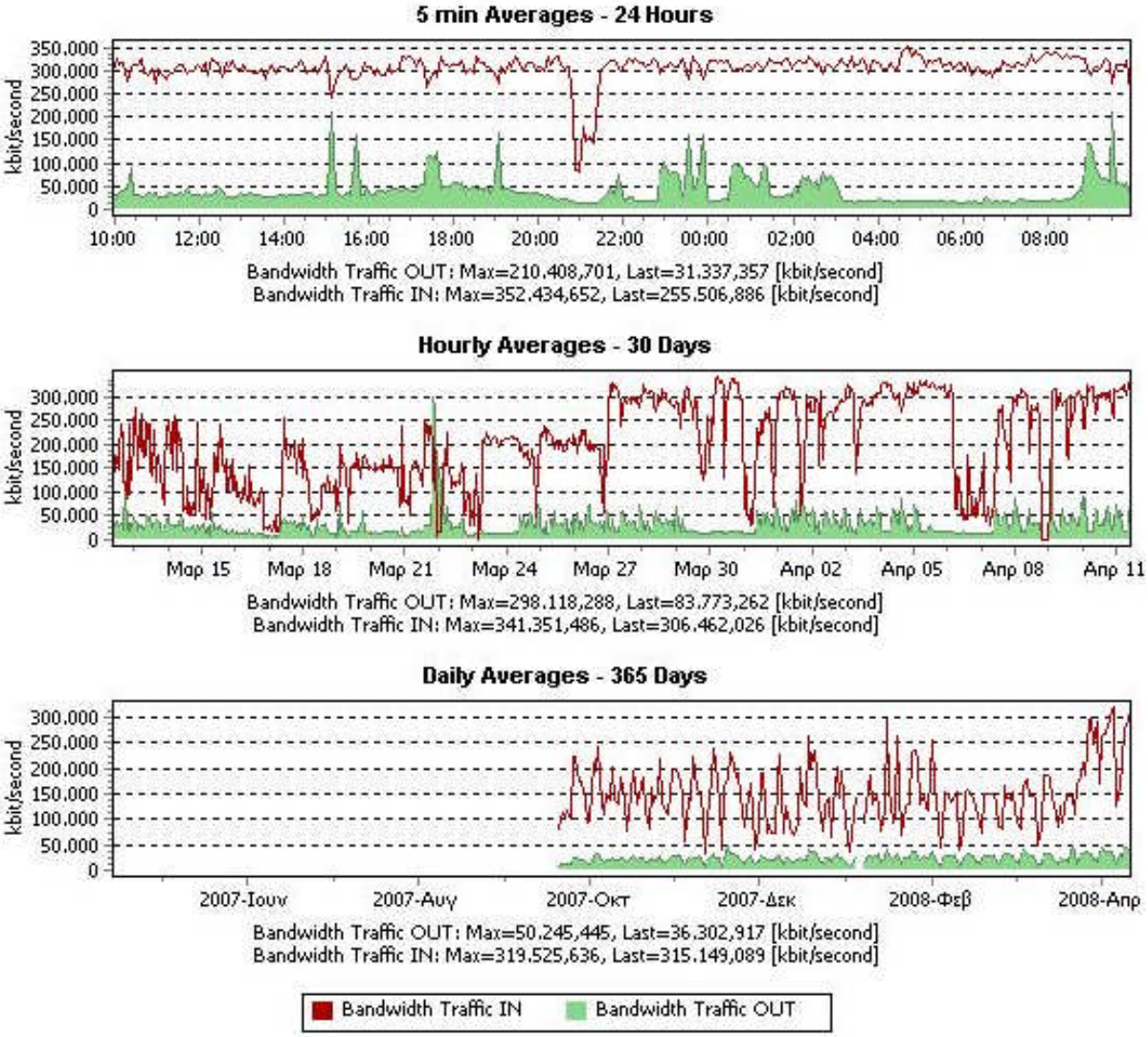
8- Troubleshooting commands

In case of issues, please run the following commands:

```
Show version
Show install all status
Show install all failure-reason
Show system internal log install
Show system internal log install details
```

12.3 Annexe 3 : Enregistrement des débits.

L'enregistrement ci-dessous représente le débit global.



12.4 Annexe 4: eAward.

Hewlett-Packard eAwards Congratulates

Philippe Duboscq

in appreciation for your outstanding efforts

Reason for Recognition

For total commitment and involvement with the extended elevation over the recent Easter Weekend. You worked long and difficult hours in a difficult environment

Nominated by: Andrew Jessop
Award Date: April 27, 2008

Note: Your participation and rights under this program will be governed solely by the rules established under the eAwards program as administered by Hewlett-Packard. This award may be subject to taxation at the time of nomination or redemption per local country tax laws; any applicable taxes will be automatically deducted from your paycheck or reported in your income statement. Please refer to the eAwards web site for policy, FAQs and more information.

12.5 Annexe 5: Fermeture officielle de l'appel

Monday, May 19, 2008

From: **Customer CEO**

To: **HP Management**

Subject: **Replication incident - formal letter of closure**

Dear Makis,

Following your letter regarding the Replication Issue, stating HP's position that the problem has been resolved and the performance of our replication facility has been tested and is currently equal or better to the one before the identification of the problem back in March, we would like to inform you that we accept to start gradually closing the technical escalation.

Please inform us about the reduced escalation level (e.g. monitoring, etc) and steps to be followed. In addition, please have in mind that we are also expecting a proposed action plan regarding the recommended, by HP, enhancements to the facility (e.g. hardware compression).

Given the opportunity I would like to thank the management and all the team members both from HP (including Competence Centers) and our organization for their commitment and huge effort towards the resolution of this incident.

Kind Regards,
Chief Executive Officer – IT Services